UCSAL
UNIVERSIDADE CATÓLICA
DO SALVADOR

LUÍZA MOURA COSTA SPÍNOLA

O TRATAMENTO DO *SPOOFING* CONFORME A LEGISLAÇÃO PENAL BRASILEIRA: UMA ANÁLISE SOBRE A TIPICIDADE DESSA TÉCNICA PARA ACESSAR CONTAS DE E-MAIL E APLICATIVOS

SALVADOR
2020

LUÍZA MOURA COSTA SPÍNOLA

O TRATAMENTO DO *SPOOFING* CONFORME A LEGISLAÇÃO PENAL BRASILEIRA: UMA ANÁLISE SOBRE A TIPICIDADE DESSA TÉCNICA PARA ACESSAR CONTAS DE E-MAIL E APLICATIVOS

Dissertação de Mestrado apresentada ao Programa de Pós-Graduação em Direito da Universidade Católica do Salvador (PPGD/UCSal), como requisito parcial para a obtenção do título de Mestre.
Linha de Pesquisa: Políticas Públicas e Efetivação dos Direitos Fundamentais

Orientador: Prof. Dr. Fábio Roque da Silva Araújo

SALVADOR
2020

Ficha Catalográfica. UCSal. Sistema de Bibliotecas

S758 Spínola, Luíza Moura Costa
O tratamento do *spoofing* conforme a legislação penal brasileira: uma análise sobre a tipicidade dessa técnica para acessar contas de e-mail e aplicativos / Luíza Moura Costa Spínola. – Salvador, 2020.
173 f.

Orientador: Prof. Dr. Fábio Roque da Silva Araújo.

Dissertação (Mestrado) – Universidade Católica do Salvador. Pró-Reitoria Pesquisa e Pós-Graduação. Mestrado em Direito. Linha de Pesquisa: Políticas Públicas e Efetivação dos Direitos Fundamentais.

1. Crimes Informáticos 2. Direito Penal Informático 3. Spoofing
I. Araújo, Fábio Roque da Silva – Orientador II. Universidade Católica do Salvador. Pró-Reitoria de Pesquisa e Pós-Graduação III. Título.

CDU 681.324:343.23

TERMO DE APROVAÇÃO

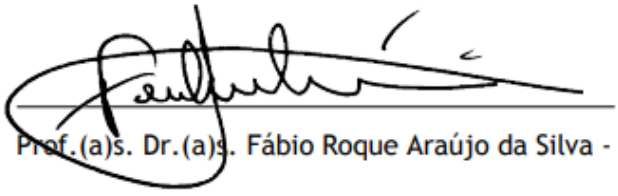
Luíza Moura Costa Spínola

"O Tratamento do Spoofing Conforme a Legislação Penal Brasileira: Uma Análise sobre a Tipicidade dessa Técnica para Acessar Contas de E-Mail de Aplicativos".

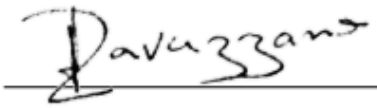
Dissertação aprovada como requisito parcial para obtenção do grau de mestre em Direito da Universidade Católica do Salvador.

Salvador, 04 de dezembro de 2020.

Banca Examinadora:



Prof.(a)s. Dr.(a)s. Fábio Roque Araújo da Silva - UCSAL (orientador)



Prof.(a) Dr.(a) Fernanda Ravazzano Lopes Baqueiro - UCSAL

Prof.(a) Dr.(a) Eduardo Viana Portela Neves – UFBA

AGRADECIMENTOS

Agradeço a Deus e aos espíritos de luz que me permitiram concluir esse trabalho

À minha família, sobretudo à minha mãe, que sempre incentivou minha vida acadêmica.

Aos meus amigos, pelo carinho e apoio constantes.

Ao meu orientador, Fábio Roque Araújo, por ter aceitado minha ideia de escrever sobre um tema tão diferente.

À professora Maria Auxiliadora Minahim, pela atenção, paciência e incentivo.

Ao professor Spencer Toth Sydow, pela inspiração concedida por meio de suas obras.

Aos professores do PPGD-UCSAL pela acolhida.

Aos meus colegas do mestrado, pela confiança por terem me escolhido como representante discente.

RESUMO

Inserida na linha de pesquisa Políticas Públicas e Efetivação dos Direitos Fundamentais, a presente dissertação tem como ponto de partida a denúncia de crimes investigados na Operação *Spoofing*. Na referida operação da Polícia Federal, apura-se o acesso desautorizado a mensagens de pessoas envolvidas na Operação Lava Jato trocadas por meio do aplicativo Telegram. O Ministério Público denunciou os réus pelo crime previsto no artigo 154, § 3º do Código Penal. Trata-se do crime de invasão de dispositivo informático, um tipo penal que busca proteger tanto a privacidade quanto a segurança informática. Esse trabalho visa elucidar que o uso de *spoofing* para acesso desautorizado a contas de e-mail e aplicativos de mensagens não pode ser considerado uma conduta criminosa nos moldes do mencionado artigo. A legislação brasileira não apresenta termos claros o suficiente para viabilizar uma interpretação à luz do princípio da legalidade. Para compreender como a tecnologia da informação evoluiu até ser incluída em práticas criminosas, será realizada uma análise do surgimento dos primeiros dispositivos até o desenvolvimento dos mecanismos mais atuais. Ademais, serão examinados os conceitos que compõem o chamado Direito Penal Informático e as iniciativas para combater a criminalidade informática. Também será feita a análise da proteção do material de cunho privado, como arquivos de texto e imagens, pelo Direito Penal brasileiro e estrangeiro. Conclui-se que ferramentas não são "dispositivos informáticos" e, na situação que ensejou a Operação *Spoofing*, também não houve violação de dispositivo informático, mas apenas o aproveitamento de uma falha no sistema do aparelho celular para acessar a caixa postal. A legislação brasileira ainda é incipiente e, para alcançar um resultado melhor quanto ao combate à criminalidade informática, deve ser elaborada por uma equipe multidisciplinar, composta não somente juristas, mas também por profissionais das áreas de Tecnologia da Informação e Comunicação.

Palavras-chave: Crimes Informáticos. Direito Penal Informático. *Spoofing*.

ABSTRACT

Aligned with the research line Inserted in the line of research Public Policies and Effectiveness of Fundamental Rights, this dissertation has as its starting point the denouncement of crimes investigated in Operation Spoofing. In this Federal Police operation, unauthorized access to messages from people involved in Operation Car Wash was verified through the Telegram application. The Public Ministry denounced the defendants for the crime provided for in article 154, paragraph 3 of Brazilian Criminal Code. The crime under discussion is denominated computer device invasion, a criminal type that aims to protect both privacy and computer security. This work aims to clarify that the use of spoofing for unauthorized access to e-mail accounts and messaging applications cannot be considered criminal conduct along the lines of the referenced article. Brazilian law does not present terms that are clear enough to enable an interpretation according to the principle of legality. In order to understand how information technology evolved until it was included in criminal practices, an analysis will be made of the emergence of the first devices until the development of the most current mechanisms. In addition, concepts that compose the Ciber Criminal Law and initiatives to combat cyber criminality will be examined. The analysis of the protection of private material, such as text and image files, will also be carried out by Brazilian and foreign Criminal Law. It is concluded that accounts of e-mail and applications are not "computer devices" and, in the situation that caused Operation Spoofing, there was also no violation of a computer device, but only the use of a failure in the cell phone system to access the cell phone's voicemail. Brazilian legislation is still incipient and, to achieve a satisfactory result in the fight against cybercrimes, it must be prepared by a multidisciplinary team, composed not only of legal experts, but also of professionals in the areas of Information and Communication Technology.

KEY WORDS: Cyber Crimes. Cyber Criminal Law. Spoofing.

SUMÁRIO

1 INTRODUÇÃO

Com o desenvolvimento dos meios de comunicação e das atividades praticadas no ciberespaço, anglicismos como “smartphone” e “*bitcoin*” passaram a ser incluídos no cotidiano das pessoas. A maior parte dos aparelhos celulares, atualmente, possui acesso à Internet, de modo que as pessoas utilizam aplicativos para desempenhar as mais diversas práticas. É possível acessar, além de e-mails e redes sociais, contas bancárias, livros eletrônicos (e-books), jogos e serviços de entrega. Tais alterações na rotina da população acabaram por gerar novas relações e demandas.

De acordo com uma frase muito conhecida no meio jurídico, o Direito é considerado o “último vagão do comboio das transformações sociais”, sendo essa máxima atribuída a Ronald Dworkin. Os responsáveis pela elaboração das leis, ao se depararem com questões como fraudes cometidas com o uso de ferramentas informáticas e invasões de gadgets, os dispositivos eletrônicos portáteis, precisam se adaptar para solucionar essas contendas. Assim, foi cunhado o termo “Direito Informático”, ou “Direito da Informática”, que repercute em vários ramos jurídicos, tais como o Direito Civil, que busca resolver dúvidas sucessórias em casos nos quais há criptoativos no patrimônio do *de cujus*, o Direito Constitucional, questionando se o acesso à Internet pode ser considerado um direito fundamental, e o Direito Penal analisando os novos bem jurídicos decorrentes do advento da sociedade da informação, para mencionar alguns exemplos.

Sobre o Direito Penal, embora já houvesse diversas questões jurídicas recorrentes à aplicação desse ramo do Direito no ciberespaço, até o final do ano de 2012 não havia no Brasil uma lei específica para criminalizar a conduta de acesso desautorizado a dispositivos informáticos. Apesar da existência de propostas já em curso, foi necessário um episódio envolvendo uma atriz consagrada para que fossem tomadas providências concretas. Trata-se de mais um caso no qual percebe-se influência da mídia sob o Poder Legislativo. A Lei nº 12.737/2012, além de ser conhecida como Lei de Crimes Informáticos, foi apelidada de “Lei Carolina Dieckmann”, por conta da atriz cuja situação levou à criação dessa norma.

Com o advento da Lei nº 12.737/2012, o Código Penal passou a incluir o tipo “invasão de dispositivos informáticos” em seu art. 154-A. A referida lei está em vigor há relativamente pouco tempo, menos de uma década, de modo que não há ainda entendimento consolidado entre os órgãos judiciais brasileiros sobre alguns de seus aspectos. No entanto, trata-se de uma

questão importante, uma vez que delitos informáticos podem lesar, além de bens jurídicos ainda pouco conhecidos pelos operadores do Direito Penal, como a segurança informática, bens jurídicos cuja proteção já é reconhecida há muito, como o direito à intimidade e o direito à privacidade.

Contudo, o legislador brasileiro não definiu expressões contidas na Lei Carolina Dieckmann como "dispositivo informático" ou "violação indevida de mecanismo de segurança". As consequências da escolha de vocábulos tão imprecisos foram percebidas alguns anos após a entrada em vigor da Lei nº 12.737/2012. Acontecimentos recentes envolvendo divulgações de mensagens trocadas em aplicativos por membros do Ministério Público e do Judiciário envolvidos na Operação Lava Jato levaram ao seguinte questionamento: o emprego da técnica denominada *spoofing* para acesso desautorizado a contas de e-mail e aplicativos de mensagens pode vir a ser considerado um crime nos termos da legislação penal brasileira?

O termo "*spoofing*" ainda é pouco difundido em áreas do conhecimento que não sejam ligadas à tecnologia da informação. O conjunto de diligências tomado pela Polícia Federal para investigar a mencionada situação foi batizado de Operação *Spoofing* por conta dessa técnica. Trata-se de um ardil, uma forma de ludibriar o titular do dispositivo informático, da conta de e-mail ou de um aplicativo para se aproveitar de brechas nos mecanismos de segurança informática e, assim, acessar uma dessas ferramentas.

A divulgação das conversas, todas realizadas entre as pessoas que atuavam na Operação Lava Jato, foi um acontecimento de tanta repercussão que a imprensa denominou o episódio de "Vaza Jato". Na denúncia[1] realizada pelo Ministério Público Federal, os responsáveis pelo acesso desautorizado aos aparelhos celulares das referidas pessoas foram acusados pelos crimes de invasão informática (art. 154-A do Código Penal), organização criminosa (art. 2º da Lei nº 12. 850/2013) e interceptação de comunicações informáticas (art. 10º da Lei nº 9.296/96).

Essa dissertação não visa a se imiscuir em questões políticas que essa situação possa suscitar. O objeto desse trabalho é elucidar que o uso de *spoofing* para acesso desautorizado a contas de e-mail e aplicativos de mensagens não pode ser considerado uma conduta criminosa nos

[1] MINISTÉRIO PÚBLICO FEDERAL. **Denúncia em face de Walter Delgatti Neto, Gustavo Henrique Elias Santos, Thiago Eliezer Martins Santos, Danilo Cristiano Marques, Suelen Priscila De Oliveira, Luiz Henrique Molição e Glenn Edward Greenwald**. Procuradoria da República no Distrito Federal, Brasília, 20 jan. 2020. Disponível em: http://www.mpf.mp.br/df/sala-de-imprensa/docs/denuncia-spoofing. Acesso em: 03 maio de 2020.

moldes do art. 154-A, pois, se assim ocorrer, estará configurado um descumprimento do princípio da legalidade. As referidas ferramentas (contas de e-mail e aplicativos de mensagens) não podem ser consideradas "dispositivos informáticos" e o emprego da técnica não envolve "violação de mecanismo de segurança", conforme os termos da referida norma.

O objetivo geral dessa dissertação é a análise da técnica de *spoofing* conforme a legislação penal brasileira capaz de abranger a criminalidade informática. Trata-se de um método que pode ser utilizado tanto para violar o bem jurídico da segurança informática quanto o da preservação da intimidade e privacidade, sendo esse último previsto em mais de uma norma vigente no ordenamento jurídico do brasileiro. Ademais, questiona-se se a utilização dessa técnica para alcançar fins similares pode se amoldar a outros tipos penais previstos na legislação brasileira, como o crime de violação de correspondência, descrito no art. 151 do Código Penal ou o crime previsto no art. 10º da chamada Lei de Interceptação Telefônica[2].

Já os objetivos específicos consistem em: descrever a evolução das ferramentas informáticas e como seu uso; investigar como os países buscam combater a criminalidade informática, em situações, além da invasão a dispositivos informáticos, que envolvam crimes transnacionais, como fraude, ciberterrorismo e propagação de conteúdo relacionado à pornografia infantil; analisar condutas criminosas de violação à intimidade e à privacidade e suas modificações nos campos legislativo e investigativo por conta do desenvolvimento das ferramentas tecnológicas; analisar como os poderes Legislativo e Judiciário, bem como os órgãos de investigação, processam certos crimes informáticos no Brasil, como o acesso desautorizado a dispositivos eletrônicos e fraudes.

Sobre a metodologia utilizada nas pesquisas, foram adotados os métodos bibliográfico e documental, utilizando, principalmente, livros e artigos das áreas jurídica e de tecnologia da informação, bem como obras de filosofia e sociologia, de maneira a chegar a um resultado em conformidade com a realidade atual, além de legislações e precedentes brasileiros e estrangeiros. Dessa forma, a abordagem empregada nesse trabalho será a qualitativa, na qual se analisa um fenômeno social, nesse caso, o uso da técnica de *spoofing* para práticas criminosas.

O primeiro capítulo desse trabalho propõe-se a tecer algumas considerações, será examinada a construção do chamado ciberespaço, desde as técnicas que auxiliaram no desenvolvimento

[2] Conforme será abordado no capítulo 6.

dos protótipos dos primeiros computadores, o estudo sobre as origens da Internet, até a criação de ferramentas e mecanismos desenvolvidos pela área da Tecnologia da Informação.

Após alguns esclarecimentos sobre o espaço cibernético, bem como de aspectos da cibercultura que demandam respostas por parte do Direito Penal, será abordada a disciplina do Direito Penal Informático. Trata-se de um sub-ramo do Direito Penal, assim como o Direito Penal Econômico. A matéria versa sobre a condutas praticadas no ambiente informático que não necessariamente são lesivas à segurança informática, mas também a outros bens jurídicos, como o patrimônio, a honra e a intimidade.

Serão também abordadas legislações de determinados países, além do Brasil, e as normas aplicadas a nível transnacional. Determinados países, como os Estados Unidos e boa parte dos países europeus, possuem legislações relativa à criminalidade informática muito mais desenvolvidas do que a brasileira. Conforme será mencionado, o Brasil até o momento não é parte do maior tratado internacional voltado ao combate a essa espécie de criminalidade, o que acaba por prejudicar a elaboração de políticas nesse sentido.

Ademais, a questão da proteção a bens jurídicos como a intimidade e a privacidade é frequentemente citada ao analisar certos crimes informáticos. Dessa forma, a história da salvaguarda desses bens jurídicos será explanada, bem como a legislação de alguns países e decisões de órgãos judiciais sobre o assunto.

Com essas explicações acerca da construção do ciberespaço e as demandas decorrentes de sua expansão, do Direito Penal Informático e da tutela penal da intimidade, será possível examinar a questão principal do trabalho. As características do uso do *spoofing*, especificamente em uma situação similar à que ensejou a Vaza Jato, serão analisadas de acordo com as normas penais vigentes no ordenamento jurídico brasileiro para verificar se é viável que o emprego da técnica para acesso a mensagens particulares seja considerado uma conduta criminosa.

2 MEIO AMBIENTE VIRTUAL: O CIBERESPAÇO

O termo “ciberespaço” foi utilizado pela primeira vez em um romance de ficção científica denominado *Neuromancer*[3], escrito no ano de 1984 pelo estadunidense William Gibson. A

[3] GIBSON, William. **Neuromancer**. São Paulo: Editora Aleph, ed. 5, 2016.

palavra é empregada para se referir ao âmbito das redes digitais, o qual seria uma zona de conflitos mundiais, bem como uma nova fronteira econômica e cultural. Na obra, alguns personagens, como o protagonista Case, conseguem adentrar fisicamente esse espaço, onde encontram construções virtuais para proteger informações secretas e conjuntos de dados cuja troca ocorre de forma extremamente veloz. Trata-se de uma das primeiras obras do gênero denominado *cyberpunk*, consistente em uma junção da informática com questões filosóficas.

Já o termo "cibercultura", conforme destaca Pierre Levy[4], seria uma manifestação no ciberespaço na qual ocorre a interconexão de diversas correntes de pensamento, produzindo, por exemplo, manifestações artísticas, destacando-se a música e a literatura, e políticas. Gómez-Diago[5], por sua vez, considera que a cibercultura abarca como um conjunto de práticas, atitudes, pensamentos e valores que crescem à medida que o ciberespaço aumenta. Para Putrov e Ivanova[6], a cibercultura seria um fenômeno social respaldado na nova relação das pessoas com equipamentos e tecnologias.

O último conceito de cibercultura adequa-se melhor ao objetivo desse trabalho, que versa sobre a análise da assimilação do *spoofing*, técnica que pode ser utilizada para fins de acesso não autorizado a um dispositivo ou ferramenta informática, pelo ordenamento jurídico brasileiro. Trata-se de um método atual que pode ser utilizado para violar um bem jurídico há muito estudado por juristas e reconhecido pela Constituição Brasileira: a privacidade. Como as pessoas estão incluindo cada vez mais a cibercultura em suas rotinas, o legislador não pode se recusar a dar uma resposta capaz de proporcionar a devida proteção do referido bem jurídico no ciberespaço.

Levy[7] define o ciberespaço como um âmbito de comunicação aberto por meio da interconexão de computadores de todo o mundo, bem como de suas memórias. Tal conceito abarca o conjunto dos sistemas da comunicação eletrônica, responsáveis por disseminar informações procedentes de fontes digitais ou que serão digitalizadas. A codificação digital é uma condicionante do caráter fluido, preciso e interativo da informação virtual, que seria o maior símbolo do ciberespaço. Em sua obra, publicada no final da década de 1990, o autor defende a ideia de que o ciberespaço seria a via de comunicação e suporte de memória mais relevante

[4] LEVY, Pierre. **Cibercultura**. São Paulo: Ed. 34, 1999, p. 92-93.
[5] GÓMEZ-DIAGO, Glória. Cyberspace and Cyberculture. In: KOSUT, M.; GOLSON, J. Geoffrey (ed.). **Encyclopedia of Gender in Media**. Thousand Oaks: SAGE Reference Publication, 2012, p. 1.
[6] PUTROV, Sergiy; IVANOVA, Galina. Cyberculture: Change and Rehabilitation the Body. **Philosophy and Cosmology**. Pereyaslav, 2018, v. 21, p. 117.
[7] LEVY, Pierre. *Op. cit.*, p. 92-93.

para a humanidade a partir do início do século XXI, previsão que, de fato, tornou-se realidade. Na época atual, praticamente todas as atividades desempenhadas pelas pessoas dependem, em algum grau, de elementos que funcionam no ciberespaço, tais como uso de meios de transporte e realização de operações bancárias[8].

O ciberespaço, no contexto das Tecnologias da Informação e da Comunicação, pode ser considerado como um local constituído por dados e elementos de comunicabilidade, conforme explicam Kadir e Judhariksawan[9]. Dessa forma, os autores entendem que o ciberespaço é um campo novo que vem sendo cada vez mais conhecido pela humanidade, como a Internet.

Gálik e Tolnaiová consideram que o ciberespaço é constituído principalmente pela Internet, mas também entendem que o termo é mais abrangente. Apesar do fato de o ciberespaço e a Internet serem considerados frequentemente locais idênticos, para os referidos autores o ciberespaço existe desde a época do descobrimento do telégrafo. Isso porque esse tipo de comunicação pode ocorrer entre duas pessoas em diferentes lugares do mundo em um espaço que não apresenta três dimensões tal qual o "espaço físico". Contudo, os autores admitem que o avanço da tecnologia proporcionou um ciberespaço mais sofisticado, no qual, além da possibilidade de se comunicar por sons, a comunicação por imagens também é viável, como ocorre no uso de programas como o Skype[10].

Os autores também buscam distinguir os termos "ciberespaço" e "realidade virtual". A segunda expressão refere-se a algo irreal, enquanto a primeira não tem o mesmo sentido, como visto. Gálik e Tolnaiová utilizam como exemplo para justificar sua tese o uso de um programa de comunicação para fazer uma chamada de voz. Nessa situação, trata-se de uma comunicação "real" que ocorre no ciberespaço, ou seja, há elementos físicos nesse processo, uma vez que é viabilizado por cabos de fibra ótica e ondas eletromagnética[11]. Dessa forma, o sentido do termo "realidade virtual" refere-se a algo construído artificialmente e que não é viável no "mundo físico", como alguns tipos de *Role Playing Game* (RPG), jogo no qual cada participante assume um personagem, praticados por meio de computadores. Já com o uso da expressão "ciberespaço" é possível designar a conexão entre objetos existentes no "mundo físico".

---

[8] *Ibidem*, p. 93.
[9] KADIR, Nadiah Khaeriah; JUDHARIKSAWAN; Maskun. Terrorism and Cyberspace: A Phenomenon of Cyber-Terrorism as Transnational Crimes. **Fiat Justisia**. Bandar Lampung, 2019, p. 334.
[10] GÁLIK, Slavomí; TOLNAIOVÁ, Sabína Gáliková. Cyberspace as a New Existential Dimension of Man. In: ABU-TAIEH, Evon. **Cyberspace**. Londres: IntechOpen, 2019, p. 1.
[11] *Ibidem*, p. 2.

O ciberespaço pode ser explicado com a sua divisão em quatro camadas, de acordo com o modelo proposto por David Clark. A camada mais externa seria onde as pessoas que fazem parte do ciberespaço se comunicam e executam tarefas, modificando assim a natureza deste. Em seguida, haveria a camada do ciberespaço na qual as informações são armazenadas, disseminadas e alteradas. A terceira parte seria constituída pela estrutura lógica responsável pela composição dos serviços oferecidos nesse âmbito, bem como por sustentar a natureza da plataforma do ciberespaço. Por fim, a camada mais interna do ciberespaço seria formada pelos fundamentos físicos que servem como suporte para os fundamentos lógicos[12].

Clark[13] esclarece que aquilo que é conhecido como ciberespaço não é uma criação do computador, mas a interconexão entre os níveis já mencionados. O autor ainda explica que, apesar de haver uma constante vinculação da ideia de ciberespaço com a Internet, é possível que existam ciberespaços alternativos criados por abordagens de interconexão distintas.

O fascínio e o espanto simultaneamente exercidos sobre o ser humano pelo ciberespaço e pela realidade virtual decorrem de sua incompletude. Isso estimula o indivíduo a imaginar projetos futuros, tornando-o ansioso por aquilo que está por vir. O entusiasmo provém de uma idealização de um futuro aberto a várias possibilidades, uma época superior ao passado e ao presente[14].

A expansão do ciberespaço também pode ser percebida como consequência de uma dinâmica iniciada pelos jovens, que enxergavam diversas possibilidades de comunicação apresentadas pela evolução da tecnologia, segundo destaca Levy. Ademais, a humanidade já vem experimentando a acessibilidade a um espaço de comunicação relativamente novo e está buscando explorar suas características positivas nos planos cultural, econômico e político. Para o autor, a desatenção por esses novos comportamentos viabilizados pela tecnologia é semelhante ao desprezo de alguns pelo *rock* quando esse estilo musical surgiu, o que não impediu seu desenvolvimento[15].

Antes de adentrar nas explanações sobre os crimes informáticos propriamente ditos, será realizado um breve histórico da criação e aprimoramento dos computadores e da Internet.

---

[12] CLARK, David. **Characterizing cyberspace: past, present and future**. Massachusetts Institute of Technology. Cambridge, 2010, p. 1.
[13] *Ibidem, loc. cit.*
[14] İLTER, Tuğrul. The Otherness of Cyberspace, Virtual Reality and Hypertext. In: ABU-TAIEH, Evon. **Cyberspace**. Londres: IntechOpen Limited, 2019, p. 635-646.
[15] LEVY, Pierre, *Op. cit*., p. 16.

Faz-se relevante explicar o contexto em que essas ferramentas surgiram e como se deu seu desenvolvimento até chegar àquilo que é conhecido hoje como ciberespaço, com uma linguagem e cultura próprias.

2.1 ADVENTO E EVOLUÇÃO DOS COMPUTADORES

Não há como ignorar o fato de que computadores se tornaram ferramentas imprescindíveis para a comunicação entre pessoas. Conforme elucida Mijwil[16], a Internet e o e-mail são capazes de manter indivíduos em contato nos lugares mais longínquos do planeta por meio do computador, instrumento que também é capaz de armazenar dados e informações e compartilhá-los em frações de segundos.

Dentre as funções que os computadores desempenham, o autor[17] destaca que tais máquinas são capazes de organizar atividades empresariais, a indústria, os transportes, bem como são fundamentais em praticamente todos os campos do conhecimento. Mas o que seria exatamente um computador? Como essas máquinas foram desenvolvidas até chegar aos dispositivos portáveis que podem acessar a Internet, como os *tablets* e os smartphones?

A definição do que seria um computador, para Berkeley[18], é uma questão de extrema importância, pois a partir dela se originam outros questionamentos, alguns até de ordem filosófica. Por exemplo: poderia o cérebro ser considerado similar a um computador? Talvez ambos sejam semelhantes, uma vez que tanto o órgão quanto o dispositivo possuem a capacidade de processar informações.

O conceito de computador tem, inclusive, consequências na esfera do Direito, afinal nem sempre a legislação de um país está clara o suficiente para definir quais dispositivos, como os *tablets* e os smartphones, podem ser objetos de invasão informática. Ademais, a precisão conceitual se faz relevante para delimitar os limites das capacidades de instrumentos considerados como computadores.

Já Höltgen questiona se o termo "computador" seria abrangente o bastante para designar calculadoras analógicas ou digitais ou se a expressão "computador doméstico" seria utilizada apenas para se referir a instrumentos não restritos às áreas científicas, econômicas ou

[16] MIJWIL, Maad M. **History of Computer**. Baghdad: University of Baghdad, mar. 2018, p. 4.
[17] *Ibidem, loc. cit.*
[18] BERKELEY, Istvan S. N. A Computational Conundrum: "What is a Computer?" A Historical Overview. **Minds and Machines**. Stuttgart, 2018, v. 28, p. 375.

militares. Para chegar a tais respostas, seria necessário recorrer a um estudo da história da tecnologia e das demandas da sociedade em geral[19].

Um computador seria uma composição específica de unidades de processamento, de transmissão, de memória e de conexões para entrada e saída de informações, segundo a concepção de Steven Levy[20]. O autor ainda explica que computadores da mesma marca podem conter peças de diversas procedências, bem como computadores de marcas distintas podem apresentar elementos bastante similares.

A palavra "computador" é empregada para designar uma máquina que processa dados por meio de um programa, de acordo com Mijwil[21]. O autor esclarece que tais máquinas são programadas de forma livre, o que quer dizer que o dispositivo processa os dados do usuário fornecendo um resultado desejado por aquele que o programou.

Para compreender como os computadores evoluíram até chegarem aos dispositivos portáveis com acesso à Internet amplamente popularizados na época atual será realizada uma análise histórica de como tais ferramentas foram desenvolvidas a partir do século XVII.

2.1.1 Máquinas de calcular: as precursoras dos computadores

O dicionário de inglês desenvolvido pela Universidade de Oxford é mencionado por Berkeley[22] para explicar a origem do termo "computador", cuja aparição se deu em 1613, tendo sido a palavra utilizada, inicialmente, para se referir a um indivíduo que realiza cálculos. No mesmo sentido, Maad M. Mijwil[23] elucida que se trata de uma palavra de procedência latina empregada para designar a função de uma pessoa que executa cálculos complexos para outros profissionais, como, por exemplo, astrônomos.

Após algum tempo, a palavra "computadores" passou a ser utilizada para se referir às pessoas que operavam calculadoras mecânicas. Em meados do século XVII, dois cientistas, o alemão Wilhem Schickard e o francês Blaise Pascal desenvolveram, de maneira independente, as

[19] HÖLTGEN, Stefan. Fifty years in home computing, the digital computer and its private use(er)s. **International Journal of Parallel, Emergent and Distributed Systems**. Londres, mar. 2019, p. 1-2.
[20] LEVY, Steven. **Hackers: Heroes of The Computer Revolution**. Nova York: Dell Publishing, 1984, p. 46.
[21] MIJWIL, Maad M., *Op. cit.*, p. 4.
[22] BERKELEY, Istvan S. N., *Op. cit*., p. 375.
[23] MIJWIL, Maad M., *Op. cit*., p. 1.

primeiras calculadoras. A ideia era proporcionar melhores ferramentas para efetuar cálculos, instrumentos que pudessem realizar essa tarefa de modo mais rápido e preciso[24].

Das duas invenções realizadas na mesma época, a de Pascal ficou conhecida "máquina de Pascal" ou "Pascalina" e foi mais popularizada do que a de Schinckard, criada em 1623, apesar de ter sido desenvolvida cerca de duas décadas depois. Ambas tinham como ponto de partida um instrumento denominado ábaco, inventado na Ásia, que consiste em um retângulo de madeira onde são manuseadas contas para viabilizar a realização de cálculos de forma mais eficiente[25].

Até a metade do século XIX foram desenvolvidas diversas máquinas com a mesma finalidade, porém nenhuma delas chegou a ser produzida em larga escala. Dentre as calculadoras idealizadas nessa época, uma das mais sofisticadas foi de autoria do inglês Charles Babbage, considerado um dos pioneiros da ciência da computação[26]. O projeto do instrumento, que ficou conhecido como "Máquina Analítica", foi apresentado ao público em 1837 e seria programável para realizar as quatro operações básicas. Ressalte-se que, no início do século XIX, o tecelão francês Joseph Marie Jacquard já havia criado um tear mecânico que usava cartões de madeira com o mesmo sistema utilizado posteriormente pelos primeiros protótipos de computadores[27].

Alguns anos depois, Babbage passou a se corresponder com Ada Lovelace, única filha legítima do poeta inglês Lorde Byron, e, assim como o inventor da "Máquina Analítica", também matemática. Lovelace envolveu-se no projeto de Babbage e criou o primeiro algoritmo para sua invenção, sendo, por esse feito, considerada a primeira programadora de computadores[28]. Atualmente, estima-se que a máquina teria funcionado, mas a construção da mesma nunca foi efetuada devido à falta de peças e de recursos financeiros[29].

Nos Estados Unidos, no final do século XIX, um sistema de cartões perfurados para realizar as operações de recenseamento da população foi criado por Hermann Hollerith[30]. Essa

[24] *Ibidem, loc. cit.*
[25] MARCOLIN, Neldson. Máquina de Calcular: Invenção do matemático francês Blaise Pascal completa 360 anos. **Pesquisa FAPESP**, ed. 75. São Paulo, 2002, p. 8-9.
[26] MIJWIL, Maad M. *Op. cit.*, p. 1.
[27] MOCHETTI, Karina. The Impact of Women in Computer Science History: A Post-War American History. **Transversal International Journal for the Historiography of Science**. Belo Horizonte, 2019, n. 6, p. 66.
[28] *Ibidem, loc. cit.*
[29] MIJWIL, Maad M, *Op. cit.*, p. 2.
[30] *Ibidem, loc. cit.*

invenção utilizava princípios similares aos que Jacquard empregou em seu tear mecânico. Tais máquinas foram aproveitadas também pela Universidade de Harvard, onde a astrônoma Henrietta Swan Leavitt foi parte de um dos primeiros grupos de "computadores" Esses grupos eram compostos, geralmente, por mulheres, pois na época não lhes era permitido operar telescópios ou outras máquinas[31].

A partir do século XX, os protótipos começaram a se aproximar dos computadores utilizados atualmente. Tal desenvolvimento ocorreu, principalmente, devido à preocupação dos Estados Unidos em criar aparatos tecnológicos mais sofisticados, principalmente após a Segunda Guerra Mundial.

2.1.2 Os Computadores no Século XX

Os computadores, tais como são conhecidos hoje, podem ser definidos como ferramentas eletromecânicas dotadas de sistemas de processamento de dados totalmente eletrônicos desenvolvidas no século XX, mais especificamente em meados da Segunda Guerra Mundial, consoante Mijwil. As estruturas que dariam origem aos futuros computadores eram, inicialmente, obras de engenharia desenvolvidas a partir da pesquisa de diversos inventores, como Konrad Zuse, um dos pioneiros da área[32].

O engenheiro alemão Zuse foi responsável pela criação de um computador binário eletromecânico chamado Z1 antes da Segunda Guerra Mundial. Entretanto, a máquina foi destruída durante um bombardeio. Durante o período da guerra, Zuse desenvolveu mais duas máquinas, porém o governo alemão não concedeu apoio às suas pesquisas. O engenheiro então fugiu para Suíça, onde obteve o respaldo necessário para continuar desenvolvendo seus projetos no Instituto Federal de Tecnologia de Zurique[33].

Além de Zuse, considera-se que Alan Turing foi um dos primeiros cientistas a contribuir com a computação em virtude de um estudo publicado por ele em 1937 sobre uma "máquina universal", conforme esclarecem Lee e Impagliazzo[34], também chamada de "máquina de Turing". A intenção do matemático britânico era criar uma máquina capaz de solucionar

[31] MOCHETTI, Karina, *Op. cit.*, p. 66.
[32] MIJWIL, Maad M, *Op. cit.*, p. 2.
[33] LEE, John A. N. **Computer Pioneers**. Los Alamitos: IEEE Computer Society Press, 1995.
[34] LEE, John A. N.; IMPAGLIAZZO, John. Using Computer History to Enhance Teaching. In: LEE, John A. N.; IMPAGLIAZZO, John. **History of Computing in Education.** Boston: Spring Science Business & Media, 2006, p. 169.

qualquer problema matemático por meio de um algoritmo. Tais estudos viabilizariam, mais tarde, um meio físico que pudesse disponibilizar a chamada inteligência artificial[35].

Turing, considerado um dos pais da computação moderna, teve um papel fundamental para ajudar o Reino Unido a vencer a guerra, pois conseguiu decifrar um código alemão denominado Enigma. Tal feito só foi possível graças à sua máquina eletromecânica, precursora dos computadores modernos, capaz de decodificar cerca de três mil mensagens militares da Alemanha por dia[36].

No início da década de 1940, a construção do *Electronic Numerical Integrator Computer* (ENIAC, Computador Integrador Eletrônico Numérico em português) foi percebida como um dos marcos da história da computação, conforme destaca Berkeley. Esse instrumento foi criado na Universidade da Pensilvânia pelos pesquisadores John Mauchly e J. Presper Eckert. Nos anos seguintes, projetos similares foram desenvolvidos, tendo esse período sido considerado de extrema importância para o desenvolvimento da computação. O ENIAC, contudo, ainda era algo bem distante dos computadores atuais: estima-se que pesava mais de trinta toneladas e ocupava um espaço de 167 metros quadrados[37].

Gugerli e Zetti explicam que, enquanto na década de 1930, o termo "computadores" era empregado para se referir às pessoas que realizavam cálculos, a partir de 1945 a palavra passou a ser utilizada para designar máquinas que desempenhavam a mesma função. Da década de 1950 em diante, os computadores tiveram seus tamanhos reduzidos, bem como os custos de sua produção[38].

Entre 1941 e 1951 foram desenvolvidos, além do ENIAC, outros computadores, como o EDVAC, BINAC e UNIVAC[39]. O sucessor do ENIAC foi o *Electronic Discrete Variable Automatic Computer* (EDVAC)[40], projeto mencionado pela primeira vez no ano de 1945 em um relatório do matemático húngaro-americano John Von Neumann. Williams[41] esclarece que o EDVAC foi a proposta inaugural de uma ferramenta para armazenamento de informações a

[35] MIJWIL, Maad M. **History of Artificial Intelligence**. Baghdad: University of Baghdad. 2015, p. 1.
[36] *Ibidem, loc. cit.*
[37] BERKELEY, Istvan S. N. *Op. cit*, p. 378.
[38] GUGERLI, David; ZETTI, Daniela. Computer history – The pitfalls of past futures. P**reprints zur Kulturgeschichte der Technik**, Zurique, 2019, n. 33, p.11.
[39] *Ibidem*, p. 10.
[40] BERKELEY, Istvan S. N. *Op. cit*, p. 375
[41] WILLIAMS, Michael R. The Origins, Uses, and Fate of the EDVAC. **IEEE Annals of the History of Computing**. 1993, v. 15, n.1, p. 23-24.

ser projetada e, por conta disso, Von Neumann seria o primeiro cientista a ter seu nome associado ao conceito moderno de computador.

O projeto do *Binary Automatic Computer* (BINAC), criado também por Eckert e Mauchly, foi lançado em 1947 e consistia em dois computadores idênticos que funcionavam simultaneamente e que possuíam em suas composições peças feitas com mercúrio e fita magnética[42]. No mesmo ano, houve o primeiro anúncio um modelo de computador no mercado estadunidense, o *Universal Automatic Computer* (UNIVAC), que só foi efetivamente concluído em 1950[43].

O desenvolvimento progressivo de peças menores foi um passo fundamental para que computadores de uso pessoal fossem viabilizados. Mijwil[44] informa que, em meados da década de 1950, os interruptores eletromecânicos e os tubos utilizados na construção de computadores foram sendo substituídos por peças de materiais mais leves e menores. Contudo, Stefan Höltgen ressalta que a utilização de computadores para fins privados não teve início somente quando as máquinas foram disponibilizadas para o público. Durante a década de 1950, estudantes do Instituto de Tecnologia de Massachusetts, considerados os primeiros hackers, e da Universidade de Stanford já usavam computadores para realizar atividades particulares[45].

Os anos posteriores à Segunda Guerra mundial até o início da década de 1960 foram uma época marcada pelos primeiros computadores desenvolvidos pela empresa estadunidense *International Business Corporation* (IBM), uma das mais antigas do ramo[46]. Entre o final dos anos sessenta até o início da década seguinte, o advento da tecnologia *Transistor Transistor Logic* (TTL) viabilizou a compactação de computadores, viabilizando a produção em massa das máquinas[47]. O TTL é uma classe de circuitos integrados utilizado com mais frequência em virtude do seu baixo custo e porque é mais confiável e rápido do que as classes

[42] INNOVATIVE Aspects of the BINAC, the First Electronic Computer Ever Sold. **Jeremy Norman's History of Science**. Disponível em: http://historyofinformation.com/detail.php?entryid=844. Acesso em: 22 jan. 2020.
[43] KEY Events in the Development of the UNIVAC, the First Electronic Computer Widely Sold in the United States. **Jeremy Norman's History of Science**. Disponível em: http://www.historyofinformation.com/detail.php?id=659. Acesso em: 22 dez. 2019.
[44] MIJWIL, Maad M. **History of Computer**, mar. 2018, p. 2.
[45] HÖLTGEN, Stefan. *Op. cit.*, p. 2.
[46] GUGERLI, David; ZETTI, Daniela. *Op. cit.*, p. 12.
[47] HÖLTGEN, Stefan, *Op. cit.*, p. 2.

anteriormente utilizadas[48]. Com a diminuição dos preços, a parcela mais abastada da população começou, assim, a ter acesso aos modelos de computadores domésticos.

A popularização, ainda que relativa, dos computadores influenciou pessoas entusiastas da ideia de desenvolver suas próprias máquinas e que, para tanto, começaram a se organizar em grupos para trabalhar nesse sentido. Parcerias muito importantes para a história da computação foram firmadas por inventores que se conheceram nesses encontros como, por exemplo, a de Steve Jobs e Steve Wozniak, fundadores da Apple. Bill Gates, fundador da Microsoft, também desenvolveu suas atividades em um desses grupos[49].

Os estabelecimentos educacionais dos EUA optaram por adquirir computadores e o ensino sobre essas máquinas acabou por entrar na matriz curricular de várias escolas no final da década de 1970. O foco dessa disciplina estava, inicialmente, na compreensão do funcionamento das peças do computador e como as instruções de execução de sua atividade poderiam afetá-lo. Isso incentivou o estabelecimento de cultura autodidata da computação, aumentando o número de pessoas interessadas no assunto[50].

Os computadores domésticos começaram a ser produzidos em uma escala maior em 1981, quando a IBM anunciou um computador para uso pessoal denominado 5150[51]. Em 1983 esse modelo foi aperfeiçoado e recebeu o nome de 5160 que, pela primeira vez, incluía um disco rígido. A nova técnica empregada nesses computadores foi chamada de XT, uma abreviatura do termo "*extended tecnology*". Os primeiros videogames, como o Atari, foram popularizados também no início dessa década[52].

Na década seguinte, o desenvolvimento dos sistemas operacionais impactou bastante as empresas que desenvolviam os computadores modernos. A Microsoft, por exemplo, estabeleceu um padrão para os computadores produzidos por ela com seu sistema denominado *Microsoft Disk Operating System* (MS-DOS) e com seus produtos da série Windows. A Apple, por sua vez, também fornecia sistemas próprios para suas máquinas. Ambos os sistemas eram projetados especificamente para os produtos das respectivas marcas. Mais tarde

[48] TRANSISTOR-Transistor Logic (TTL). In: **Technopedia**. Edmonton: Janalta Interactive, 2016. Disponível em: https://www.techopedia.com/definition/3057/transistor-transistor-logic-ttl. Acesso em: 02 de maio de 2020.
[49] MIJWIL, Maad M, *Op. cit.*, p. 3.
[50] HÖLTGEN, Stefan, *Op. cit.*, p. 8.
[51] BERKELEY, Istvan S. N., *Op. cit.*, p. 379.
[52] HÖLTGEN, Stefan, *Op. cit.*, p. 8.

surgiu o sistema operacional Linux, tornando-se uma alternativa aos sistemas padronizados oferecidos pela Microsoft e pela Apple[53].

O Linux, sistema criado no início da década de 1990 pelo engenheiro Linus Torvalds, pode ser utilizado em computadores, smartphones, *tablets* e outros dispositivos, como caixas de banco eletrônicos[54]. Diferentemente dos sistemas operacionais da Apple e da Microsoft, o Linux não foi criado visando objetivos comerciais, de modo que qualquer usuário pode criar e difundir arquivos a partir dele. A vantagem do Linux é que a maior parte dos vírus existentes na Internet não consegue afetá-lo, uma vez que a maioria dos *malwares* é desenvolvida para atacar sistemas da Apple ou Microsoft, mas é preciso ressaltar que essa característica não o faz imune a ameaças que circulam na rede mundial de computadores[55].

O fator responsável pelo avanço da portabilidade de computadores e outros dispositivos informáticos foi a expansão da Internet. Berkeley[56] destaca que o lançamento do IPhone pela Apple em 2007 foi considerado um marco no mercado de massa da computação. No ano seguinte foi lançado um celular similar com o sistema operacional Android, do Google. Esses dispositivos são chamados smartphones (telefones inteligentes, em tradução livre), pois viabilizam o acesso à Internet e e-mails. Também são chamados de dispositivos inteligentes os *tablets* e os demais que permitem essa conectividade.

Tais dispositivos foram aperfeiçoados com o passar dos anos, tendo a Apple, em 2010, lançado um produto que até então não possuía um similar no mercado: o IPad. O aparelho apresentado combinava todas as facilidades do IPhone, juntamente com mais recursos audiovisuais, e mais possibilidades de instalação de aplicativos. Embora não tenha sido o primeiro *tablet*, computador pequeno e de superfície plana operado por meio de toques na tela, o advento do IPad certamente foi um fato que movimentou o mercado desse ramo[57].

---

[53] BERKELEY, Istvan S. N., *Op. cit.*, p. 380.
[54] LINUX. In: **Encyclopaedia Britannica**. Disponível em: https://www.britannica.com/technology/Linux. Acesso em: 13 abril 2020.
[55] KURTZ, João. Linux: Linux: Tudo o que você precisa saber antes de começar a usar. **TechTudo**, 24 mar. 2015. Disponível em: https://www.techtudo.com.br/noticias/noticia/2015/03/linux-tudo-o-que-voce-precisa-saber-antes-de-comecar-usar.html. Acesso em: 13 abril de 2020.
[56] BERKELEY, Istvan S. N., *Op. cit.*, p. 380.
[57] THE Apple iPad is released. **Computer History Museum**. Disponível em: https://www.computerhistory.org/timeline/2010/. Acesso em: 23. dez. 2019.

Sobre esse fato, Crespo [58] destaca que esses novos equipamentos eletrônicos, mais especificamente os que viablizaram a utilização de aplicativos, transformaram não somente a maneira como a população se comunica, mas também como as pessoas desempenham suas atividades profissionais. De acordo com uma matéria divulgada no portal de notícias G1[59], a utilização de aplicativos de trocas de mensagens, como o WhatsApp, triplicou e voltados à produtividade, como o Evernote cresceu 115% no ano de 2013.

Em agosto de 2015 houve uma notícia de que operadoras de celular estavam preparando uma petição para ser entregue à Agência Nacional de Comunicações (ANATEL) contra o funcionamento do WhatsApp. As empresas questionariam no suposto documento acerca do serviço de voz do WhatsApp, pois elas são obrigadas a pagar à ANATEL por cada número de celular, enquanto o aplicativo estaria isento[60].

Ademais, no mesmo ano, o chamado "Efeito WhatsApp", juntamente com a crise econômica, extinguiu cerca de dez milhões de linhas de celular no Brasil, conforme outra matéria do G1. As empresas do ramo consideram que essa diminuição se deve ao fato de que as pessoas estão preferindo utilizar esse aplicativo de mensagens a manter mais de uma conta de celular. Esse fato demonstra uma preferência crescente do público pelo uso de Internet na telefonia móvel[61].

Apesar de esforços das operadoras de celular para conter a popularização do WhatsApp, o uso do aplicativo no Brasil cresceu com o passar dos anos. Com base na política de "se não pode com eles, junte-se a eles", as empresas firmaram parcerias com o WhatsApp para oferecer pacotes de serviço com uso ilimitado do aplicativo de mensagens. Esse fato demonstra como

[58] CRESPO, Marcelo Xavier de Freitas. Sobre o acesso a dispositivos digitais sem autorização judicial em situações de flagrante delito. In: PINHEIRO, Patrícia Peck. **Direito Digital 3.0 Aplicado**. São Paulo: Thompson Reuters, 2018, p. 91.

[59] USO de apps de bate-papo triplica em 2013, diz consultaria. **G1**, 13 jan. 2014. Disponível em: http://g1.globo.com/tecnologia/tem-um-aplicativo/noticia/2014/01/uso-de-apps-de-bate-papo-triplica-em-2013-diz-consultoria.html. Acesso em: 22 dez. 2019.

[60] FELITTI, Guilherme. Por que as operadoras brasileiras entraram em guerra contra o WhatsApp. **Época Negócios**, 16 dez. 2015. Disponível em: https://epocanegocios.globo.com/Informacao/Dilemas/noticia/2015/12/por-que-operadoras-brasileiras-entraram-em-guerra-contra-o-whatsapp.html. Acesso em: 23 dez. 2019

[61] GOMES, Helton Simões. 'Efeito WhatsApp' e crise 'matam' 10 milhões de linhas de celular no Brasil. **G1**, 08 dez. 2015. Disponível em: http://g1.globo.com/tecnologia/noticia/2015/12/efeito-whatsapp-e-crise-matam-10-milhoes-de-linhas-de-celular-no-brasil.html. Acesso em 10 dez. 2019.

as empresas precisam se adaptar ao mercado conforme a evolução dos dispositivos informáticos[62].

Da década de 1990 em diante percebe-se que a evolução dos computadores e dos dispositivos portáteis esteve diretamente ligada ao aumento da conectividade da população à Internet. Ocorre que o aperfeiçoamento da Internet não foi acompanhado por iniciativas suficientes para ensinar à população como utilizar a rede mundial de computadores, o que contribuiu para o aumento de riscos nesse ambiente. Apesar da popularização dessa rede ser relativamente recente, a história da Internet remete ao início do século XX, conforme será explanado na subseção seguinte.

2.2 CRIAÇÃO E DESENVOLVIMENTO DA INTERNET

A palavra "Internet" é o resultado da fusão entre as palavras da língua inglesa "*interconnected*" e "*networks*", que em português são equivalentes aos termos "interligado" e "rede", conforme lecionam Antunes e Rodrigues [63]. Em suma, a Internet seria uma infraestrutura destinada a interligar redes de computadores a nível global.

O entendimento acerca de como a Internet causou mudanças profundas na sociedade só é viável após analisar seu início até seu estado atual, segundo Raphael Cohen-Almagor. O autor elucida que a tecnologia avançou bastante em cinquenta anos, uma vez que mais demandas surgiram por parte da população e isso acarretou a criação de ferramentas informáticas para resolver essas questões. Programas para compartilhamento de arquivos e redes sociais, por exemplo, não eram sequer concebidos na etapa primordial da Internet, porém foram desenvolvidos posteriormente em virtude das necessidades dos usuários[64].

A Internet é descrita com frequência como um "caos organizado", consoante explica Marson, sendo possível empregar as mesmas palavras para explicar a história da mesma, uma vez que a Internet surgiu em um contexto no qual se temia a ocorrência de uma guerra nuclear. Os Estados Unidos tinham tanto receio quanto à expansão do Comunismo que buscaram investir boa parte de seus recursos em um canal de comunicação que fosse seguro contra ataques

[62] TRINDADE, Rodrigo. Como WhatsApp foi de inimigo a queridinho das operadoras. **Uol**, 05 jun. 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/06/05/tentaram-parar-inovacao-como-whatsapp-matou-sms-e-deu-licao-a-operadoras.htm. Acesso em: 23 dez. 2019.
[63] ANTUNES, Mário; RODRIGUES, Baltazar. **Introdução à Cibersegurança: A Internet, os Aspectos Legais e a Análise Digital Forense.** FCA – Editora de Informática Ltda.: Lisboa, 2018, p. 6.
[64] COHEN-ALMAGOR, Raphael. Internet History. **International Journal of Technoethics**. Hershey, v. 2, n. 2, 2011, p. 46.

nucleares. Com efeito, a ideia dos especialistas em táticas militares era desenvolver uma ferramenta que não apenas resistisse a tais ataques, mas também que pudesse identificá-los. A idealização de tal projeto teve início durante o governo do presidente Dwight D. Eisenhower[65].

Com o lançamento do primeiro satélite artificial desenvolvido pela União das Repúblicas Socialistas Soviéticas (URSS), em 4 de outubro de 1957, por meio do programa Sputnik, os Estados Unidos perceberam a necessidade de reagir frente ao bloco socialista, de acordo com Cohen-Almagor. Foi criada então a *Advanced Research Projects Agency* (ARPA, Agência de Projetos de Pesquisa Avançada em tradução livre para o português) em fevereiro de 1958.[66]

A preocupação dos Estados Unidos em dedicar tantos recursos ao desenvolvimento de tecnologia para ser utilizada na área militar devia-se a uma teoria dos cientistas do Departamento de Defesa do país[67]. Eles acreditavam que, se a URSS podia lançar satélites, ela também teria a capacidade de lançar mísseis nucleares.

Ocorre que as redes de comunicação existentes na época contavam com apenas um controle central, o que as tornavam vulneráveis, pois se o ponto central fosse danificado a ponto de perder sua capacidade de funcionamento, toda a rede ficaria inutilizada. A intenção dos pesquisadores era de desenvolver uma rede que pudesse ser preservada, ainda que um dos seus centros de controle fosse atacado, para que a comunicação fosse mantida e, por conseguinte, as informações não se perdessem[68].

Houve então experiência financiada pelo governo e desenvolvida pela ARPA por meio de um de seus setores, o *Information Techniques Office* (IPTO, Escritório de Técnicas de Processamento de Informações), que resultou em uma técnica de comunicação eletrônica entre computadores, denominada ARPANET, segundo explicam Fiorillo e Conte[69]. O processo de criação dessa rede de comunicação se intensificou em 1962, quando um funcionário do *Massachusetts Institute of Technology* (conhecido pela sigla MIT, trata-se, em tradução livre para o português, do Instituto de Tecnologia de Massachusetts) chamado

---

[65] MARSON, Stephen M. A. Selective History of Internet Technology and Social Work. **Journal of Technology in Human Services**. v. 14, 1997, p. 36.
[66] COHEN-ALMAGOR, Raphael, *Op. cit.*, p. 46.
[67] *Ibidem*, p. 47.
[68] *Ibidem, loc. cit.*
[69] FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari**. Crimes no Meio Ambiente Digital e a Sociedade da Informação**, 2ª ed., Saraiva: São Paulo, 2016, p. 14.

Joseph Licklider elaborou os chamados memorandos *On-Line Man Computer Comunication* (Comunicação On-Line entre Homens e Computadores)[70].

Licklider foi o primeiro diretor do Escritório de Técnicas de Processamento de Informações e tinha como uma de suas funções executar projetos para conectar os principais computadores do Departamento de Defesa entre si. O cientista foi o responsável por criar o embrião da Internet, pois acreditava na criação de uma rede mundial de computadores por meio da qual qualquer pessoa em qualquer lugar poderia ter acesso a informações e programas. Essa rede de comunicação, dessa maneira, seria uma ferramenta essencial para permitir o intercâmbio de conhecimentos científicos[71].

O projeto dos memorandos foi implementado, primeiramente, em dois centros universitários do estado da Califórnia e um no estado de Utah, viabilizando a telecomunicação entre eles. Essa técnica foi desenvolvida pelo IPTO com o objetivo final de viabilizar a comunicação entre repartições militares de forma que fosse assegurado o sigilo das informações[72]. Na década de 1970 ocorreu a primeira ligação dessa rede por satélite à Europa e, a partir desse evento, novas redes foram se interligando, a maioria nos Estados Unidos e no continente europeu[73].

No início da referida década, ocorreu um crescimento mais expressivo da ARPANET. Em outubro de 1972 houve a primeira Conferência Internacional sobre Computadores e Comunidades em Washington[74]. Nesse evento ocorreu a primeira exibição pública da ARPANET para cerca de mil pessoas. Cerca de dez anos depois, foi desenvolvido o modelo de comunicação padrão da Internet. No ano de 1974 os cientistas Vint Cerf e Robert Kahn desenvolveram um conjunto de protocolos denominado TCP/IP (sigla para a denominação *Transmission Control Protocol/Internet Protocol*) que viabiliza o estabelecimento de uma rede para conectar vários equipamentos. O termo "Internet" foi utilizado pela primeira vez nesse mesmo ano no artigo elaborado por Kahn e Cerf sobre o TCP/IP. Enquanto o TCP

[70] LEAL, Luziane de Figueiredo Simão. **Os Crimes contra os Direitos da Personalidade na Internet: Violações e Reparações de Direitos Fundamentais nas Redes Sociais**. Juruá: Curitiba, p. 76.
[71] COHEN-ALMAGOR, Raphael. *Op. cit.*, p.47.
[72] LEAL, Luziane de Figueiredo Simão. *Op. cit.*, p. 15.
[73] ANTUNES, Mário; RODRIGUES, Baltazar. *Op. cit.*, p. 4.
[74] MARSON, Stephen M. A. *Op. cit.*, p. 36.

apresenta regras para que os computadores de uma rede estabeleçam e interrompam conexões, o IP inclui regras para rotear pacotes de dados individuais[75].

A partir da criação desses protocolos a ARPANET se expandiu tanto que, em 1983, foi dividida em duas: a MILNET, utilizada por sites militares, e a ARPANET, empregada para tráfego de informações não militares. Essa divisão marcou uma etapa de crescimento da ARPANET, com a participação de universidades, centros de pesquisa e das instituições públicas dos Estados[76]. A Internet veio a partir da ARPANET, com respaldo na noção de que poderiam ser criadas diversas redes independentes com modelos distintos[77]. Ainda durante essa década, a Internet começou a ser utilizada no Brasil, mais especificamente na Universidade de São Paulo (USP). Um dos professores da instituição, Oscar Sala, desenvolveu um projeto de comunicação entre universidades a nível internacional, para permitir o intercâmbio de informações com o uso de uma rede de computadores[78].

Na década seguinte, a Internet já contava com um nível mais elevado de globalização, o que acarretou o surgimento de um dos seus mais relevantes serviços da Internet: o *World Wide Web* (WWW, Rede Mundial de Computadores em tradução livre para o português). Esse sistema foi desenvolvido pelo físico inglês Timothy John Berners-Lee e, com o advento dos primeiros programas de computador, o WWW foi ampliado até tornar-se a atual rede mundial de computadores[79]. Em 1993, o Brasil começou a implementar a Internet em seu território, tendo os Ministérios das Comunicações e da Ciência e Tecnologia autorizado o uso comercial na rede três anos depois[80].

Com a progressiva diminuição dos custos de produção dos dispositivos informáticos, a Internet tornou-se mais acessível a pessoas com menos poder aquisitivo, caracterizando um fenômeno denominado inclusão digital. Segundo informações disponibilizadas pelo portal de notícias G1, cerca de setenta por cento da população brasileira tem acesso à Internet atualmente[81].

---

[75] COHEN-ALMAGOR, Raphael. *Op. cit*., p. 50.
[76] ANTUNES, Mário; RODRIGUES, Baltazar. *Op. cit*, p. 5.
[77] COHEN-ALMAGOR, Raphael. *Op. cit*., p.50.
[78] FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. *Op. cit.*, p. 16.
[79] *Ibidem, loc. cit.*
[80] *Ibidem, loc. cit.*
[81] LAVADO, Thiago. Uso da Internet no Brasil Cresce e 70% da População está Conectada. **G1 – O Portal de Notícias da Globo**, 28 ago. 2019. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2019/08/28/uso-da-internet-no-brasil-cresce-e-70percent-da-

Apesar de o mercado da Internet demonstrar sinais de saturação em países da Europa e nos Estados Unidos, de acordo com Malaquias, ainda há espaço de crescimento para países em desenvolvimento como o Brasil e outros da América Latina, em razão do número crescente de consumidores desse serviço. Outros países que também vêm apresentando índices cada vez mais altos de consumo de Internet são a Índia e a Indonésia. Conforme o autor, o país que apresenta o maior número de usuários de Internet é a China, contando com aproximadamente 650 milhões de pessoas que se valem dessa rede, seguida pelos Estados Unidos e pela Índia, que, em breve, deverá superar os estadunidenses por conta do interesse cada vez maior da população pela rede[82].

Percebe-se que o desenvolvimento de dispositivos com acesso à Internet e o crescente número de usuários da rede transcende o uso das atividades rotineiras. Há uma mudança intensa em conceitos sociais já estabelecidos, segundo Fiorillo e Conte[83], como as relações humanas e interligando a tecnologia da informação com diversas vertentes culturais, econômicas e sociais.

A Internet, inclusive, já está substituindo meios de entretenimento utilizados antes com mais frequência, como, por exemplo, a televisão e o cinema, conforme destacam os autores[84], sendo esse fenômeno denominado efeito-substituição. As pessoas vêm utilizando a Internet para consumir músicas e vídeos, participar de eventos virtuais e se comunicar por meio de redes sociais, condutas praticadas com o intuito de se divertir, sem precisar interagir com a comunidade na qual estão inseridas presencialmente.

É possível considerar que a interação entre os indivíduos está ocorrendo mais frequentemente por meio das redes sociais do que pessoalmente. Leal[85] esclarece que essas redes foram criadas na década de 1980 a partir dos chamados *Bulletin-Board-System* (BBS), sistemas que viabilizavam o intercâmbio de dados e mensagens entre usuários de uma mesma plataforma. Os perfis pessoais sugiram a partir da década de 1990, sendo possível, por meio deles, divulgar eventos e trocar mensagens públicas e privadas.

---

populacao-esta-conectada.ghtml. Acesso em: 26 nov. 2019.

[82] MALAQUIAS, Roberto Antônio Darós. **Crimes Cibernéticos e Prova: a Investigação Criminal em Busca da Verdade**. Curitiba: Juruá, p. 46-47.

[83] FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. *Op. cit.*, p. 18.

[84] *Ibidem*, p. 26.

[85] LEAL, Luziane de Figueiredo Simão. *Op. cit*. 84-85.

Tais ferramentas que fomentaram a comunicação e o acesso à informação por meio da Internet tornaram-na um elemento fundamental no progresso das sociedades, conforme ressaltam Antunes e Rodrigues. Uma demonstração desse fato são os mecanismos recentemente implementados na Internet, como a computação na *cloud* (nuvem) e abrangência da Internet a todos os dispositivos e objetos ligados entre si e à própria rede. Dessa maneira, a Internet mantém as bases com as quais foi criada, como a ideia de acesso livre e descentralizado à informação, mas a sua situação atual é bem mais extensa, pois inclui não somente os computadores, mas todos os dispositivos eletrônicos conectados à Internet por qualquer meio físico[86].

A Internet pode ser compreendida como um suporte composto por três elementos: trata-se de uma sucessão de redes interligadas entre si com existência está a nível global, sendo um sistema no qual a comunicação entre os equipamentos se dá mediante a mesma linguagem. Esses três aspectos viabilizam a circulação de informações por intermédio de conversões de sequência. Além disso, uma das razões que levou a Internet a se tornar tão popular é que essa ferramenta de comunicação constitui, ao menos em tese, uma sociedade bastante democrática, pois todos os indivíduos com acesso à Internet seriam iguais. Pode-se considerar ainda que as regras ou limitações existentes no meio virtual ainda são bem poucas[87].

Sobre a forma da infraestrutura da Internet, Antunes e Rodrigues consideram que se trata de uma infraestrutura física na qual ocorre a comunicação entre as redes que a constituem que podem ser domésticas ou corporativas. Cada rede é formada por diversos equipamentos terminais, tais como computadores pessoais, computadores portáteis e servidores conectados por meio de *switches* e acessam a Internet através de um roteador, um equipamento de interligação. Tais instrumentos garantem que os dados sejam enviados pelos equipamentos terminais para a Internet e são inerentes à infraestrutura de comunicações. A ligação desses equipamentos é feita por meio de cabos de fibra ótica e cobre, que se localizam em espaços denominados *datacenters*[88].

O valor desses equipamentos que viabilizam o uso da Internet vem se tornando cada vez mais módico, resultando em um número crescente de usuários. Assim, é possível considerar que a popularização da Internet acarretou uma profunda transformação na sociedade como um todo,

---

[86] ANTUNES, Mário; RODRIGUES, Baltazar. *Op. cit.*, p. 5-6.
[87] SYDOW, Spencer Toth. **Crimes Informáticos e Suas Vítimas**. 2 ed., São Paulo: Saraiva, 2015, p. 31-32.
[88] ANTUNES, Mário; RODRIGUES, Baltazar. *Op. cit*., p. 6-7.

especialmente no que tange às questões de privacidade e de conceder um novo significado aos espaços, conforme destaca Leal. A interatividade é uma característica dessa ferramenta de comunicação que é muito mais abrangente do que em outros meios de comunicação. A autora cita como exemplo o fato de um indivíduo manifestar a sua opinião na Internet e tomar conhecimento da opinião alheia simultaneamente. Considera-se, assim, que a Internet serviu como meio de consolidação do direito à liberdade de expressão e o direito ao acesso à informação[89].

Essas características inerentes à Internet tornam o espaço cibernético ou ciberespaço um ambiente no qual é mais difícil estabelecer um "centro de comando", conforme lecionam Fiorillo e Comte[90], semelhante ao que existe no espaço físico. Sydow[91] ressalta que, em termos, não há cessão de parte da liberdade virtual do usuário da Internet em favor de uma autoridade central, que comanda e limita as atividades desempenhadas nesse âmbito.

2.2.1 Cibersegurança

Devido ao elevado número de equipamentos ligados e sua diversidade, assim como o índice cada vez mais alto de usuários de Internet, o espaço cibernético tem se tornado mais complexo e carente de mecanismos que viabilizem a monitoração, a vigilância e a resiliência da segurança e dos dados do usuário, segundo elucidam Antunes e Rodrigues[92]. A Internet vem transformando-se em um espaço mais inseguro para a comunicação, compartilhamento de informações e trabalho colaborativo.

Para proteger as redes, os computadores, os programas e os dados de ameaças, foram desenvolvidos tecnologias, processos e práticas, formando um conjunto de ferramentas da chamada cibersegurança[93]. Houve um aumento do uso de sistemas mais modernos, que apresentam uma maior conectividade, e, por conta dessa característica, tais sistemas ficam mais expostos a ciberataques[94]. A elevação do risco quanto à cibersegurança deve-se a vários fatores, como programas de segurança inadequados e evolução da complexidade dos ataques.

---

[89] LEAL, Luziane de Figueiredo Simão. *Op. cit*., p. 75.
[90] FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. *Op. cit.*, p. 17.
[91] SYDOW, Spencer Toth. *Op. cit*., p. 31-32.
[92] ANTUNES, Mário; RODRIGUES, Baltazar. *Op. cit*., p. 3.
[93] *Ibidem, loc. cit*.
[94] REEGÅRD, Kine; BLACKETT, Claire; KATTA, Vikash. The Concept of Cybersecurity Culture. **Proceedings of the 29th European Safety and Reliability Conference**. Singapore: Research Publishing, 2019, p. 4039.

Taddeo[95] menciona que o relatório de riscos elaborado pelo Fórum Econômico Mundial incluiu os ciberataques como um dos dez maiores riscos de impacto global. A cada ano os dados sobre ciberataques e seus impactos demonstram que eles são uma ameaça crescente à sociedade da informação. A partir dessa divulgação do Fórum Econômico Mundial, chegou-se a duas conclusões. A primeira é incontroversa: infraestruturas digitais são porosas, ou seja, é bastante provável que apresentem algum tipo de brecha para um ciberataque. A segunda dedução da autora é que a cibersegurança pode ser considerada um bem de interesse público[96].

Assim, torna-se essencial para a sobrevivência de todas as organizações no âmbito do ciberespaço providenciar mecanismos de segurança. Empresas públicas e bancos, por exemplo, estão investindo bastante em aparatos tecnológicos nesse sentido com o fim de proteger suas informações e dados pessoais de consumidores, conforme Ljubomir Lazic. Os setores mais suscetíveis de sofrerem ciberataques, segundo o autor, são aeroportos, indústrias que lidam com petróleo e hospitais. É possível que um ataque nesse sentido seja interpretado como uma ameaça à segurança nacional ou internacional quando dirigido a infraestruturas críticas. Dessa forma, a cibersegurança pode ser considerada como um assunto de interesse público, não apenas para um Estado especificamente, mas a nível mundial[97].

Os termos cibersegurança e segurança da informação são constantemente empregados como sinônimos na literatura especializada, segundo Reegård, Blackett e Katta. De acordo com os autores, a segurança da informação é a proteção dos dados, que podem ser considerados como bens, de prejuízos causados por ataques. Já a cibersegurança não é somente a proteção do ciberespaço, mas também a preservação das informações pessoais que se encontram nele. Enquanto no campo da segurança da informação, o papel que o ser humano desempenha relaciona-se com o processo de segurança, no âmbito da cibersegurança o indivíduo pode figurar como um alvo em potencial para ciberataques[98].

Além das expressões retromencionadas, o termo *Deep Web* é constantemente utilizado nos campos da informática e da tecnologia da informação. Para explicá-lo, é preciso recorrer às informações já citadas sobre a *World Wide Web* (WWW), um imenso sistema que consiste em

---

[95] TADDEO, Mariarosaria. Is Cybersecurity a Public Good?. **Minds and Machines - Journal for Artificial Intelligence, Philosophy and Cognitive Science**. Oxford, 2019, v. 29, p. 349.
[96] *Ibidem*, p. 350.
[97] LAZIC, Ljubomir. Benefit From AI In Cybersecurity. **The 11th International Conference on Business Information Security (BISEC-2019).** Belgrado, Sérvia, out. 2019.
[98] REEGÅRD, Kine; BLACKETT, Claire; KATTA, Vikash. *Op. cit*., p. 4037.

diversos servidores e usuários que têm acesso ao conteúdo vinculado a ele[99]. Os servidores conservam o conteúdo na rede por meio de páginas que contém textos, imagens, material audiovisual, gráficos e animações.

2.2.2 As Camadas da Internet

A WWW pode ser dividida em três categorias, de acordo com a acessibilidade do conteúdo da rede. Existe a *Surface Web* (rede da superfície em português), que é a porção mais aparente da WWW, a rede aberta dos usuários. Essa parte do conteúdo é de livre acesso de qualquer lugar sem barreira alguma. Tais páginas da WWW podem ser buscadas com bastante facilidade, sendo inclusive inseridos em ferramentas de pesquisa como as dos sites Bing, Google e Yahoo[100].

Já *Deep Web* (em português a expressão pode ser traduzida como "rede profunda") seria a parte intermediária da WWW que, diferente da *Surface Web*, não é indexada por sites de busca, uma vez que seu conteúdo não está em HTML, a codificação utilizada para desenvolver sites[101]. Por conseguinte, não são todos os usuários da Internet que têm acesso a essa porção da WWW. A expressão *Deep Web* foi utilizada pela primeira vez em um trabalho denominado "*The Deep Web: Surfacing Hidden Value*"[102].

O nome dessa parte da WWW deve-se ao fato de que os usuários de Internet que têm acesso a ela comparam-na com um grande iceberg, pois a parte visível da rede é apenas quatro por cento do total do conteúdo dos servidores. Os outros 96% não são acessíveis, tendo esse conteúdo sido um assunto constantemente especulado pelo público que tem interesse pelo assunto[103].

Gallardo-Rosales[104] define a *Deep Web* como uma parte da rede composta por informações, materiais e sites que não são mostradas nas ferramentas de busca disponíveis. O autor menciona que, conforme dados da Universidade da Califórnia, a *Deep Web* contém por volta de 91.000 *terabytes* de informação.

---

[99] PRASAD, M. R. Murali. Deep Web: Librarian's Perspective. **PEARL - A Journal of Library and Information Science**. Hyderabad, out.-dez. 2017, v. 11, n. 4, p. 418.
[100] *Ibidem, loc. cit.*
[101] *Ibidem, loc. cit.*
[102] BERGMAN, Michael K. **The Deep Web: Surfacing Hidden Value**. Sioux Falls: Bright Planet, 2001.
[103] GALLARDO-ROSALES, Rodolfo. **La Deep Web**. Disponível em: http://gallardo.mx/wp/?p=2391. Acesso em: 11 dez. 2019.
[104] *Ibidem, loc. cit.*

Pessoas que fazem parte do público leigo em informática por vezes questionam a razão da existência da *Deep Web*. Gallardo-Rosales explica que essa parte da web é necessária porque governos e organizações, como bancos, por exemplo, devem possuir suas informações na rede, mas assegurando o seu sigilo. No caso de um banco, diversos dados dos seus clientes estão disponíveis na rede, mas somente em uma parte dela que não pode ser acessada por qualquer um, apenas por meio de um programa criado com esse objetivo desenvolvido especificamente para o banco em questão[105].

Com alguma frequência o termo "*Deep Web*" é confundido com "*Dark Web*" (rede obscura em português). A última expressão é utilizada para se referir a uma parte da *Deep Web* que consiste em uma rede cujas informações são processadas com o uso de algoritmos existente entre os Servidores Tor[106] e seus usuários[107]. A *Dark Web* também é conhecida pelos nomes de "*Hidden Web*" ou "*Hidden Internet*" e, além do software Tor, pode ser acessada por meio da rede I2P. Ambas as ferramentas garantem que o IP do usuário seja ocultado, de modo que a sua localização física não possa ser determinada[108].

O software *Tor* viabiliza o acesso a uma infraestrutura de comunicação anônima em uma rede pública[109]. As ferramentas do *Tor* apresentam URLs[110] que terminam em "*.onion"*, uma técnica de roteamento que apresenta diversas camadas de criptografia, semelhantes a uma cebola, por isso o nome do método, garantindo assim o anonimato do usuário[111].

A *Dark Web* expandiu-se bastante na segunda década do século XXI, com o advento de mercados online anônimos que utilizam o *bitcoin*. De acordo com informações contidas no site *Bitcoin.org* [112], originalmente criado pelos dois primeiros desenvolvedores dessa ferramenta, Satoshi Nakamoto e Martti Malmi, o *bitcoin* funciona como dinheiro no âmbito da Internet, sob o ponto de vista do usuário. Trata-se da concretização da ideia de criptomoeda, uma forma de dinheiro que emprega a criptografia para controlar sua criação de

---

[105] *Ibidem, loc. cit.*
[106] *Tor* é a abreviação de *The Onion Router*.
[107] GALLARDO-ROSALES, Rodolfo. *Op. cit*. Disponível em: http://gallardo.mx/wp/?p=2391. Acesso em: 11 dez. 2019.
[108] BARATT, Monica J.; ALDRIDGE, Judith; MADDOX, Alexia. **The SAGE Encyclopedia of the Internet.** Thousand Oaks: SAGE Publications, Inc, 2018, p. 185.
[109] VERVERIS, Vasilis. Demistifying the Dark Web. **XRDS**. Nova York, 2018, v.24, n.4, p. 16
[110] Sigla de "*Uniform Resource Locator*" (Localizador Padrão de Recurso), endereço de um recurso disponível em uma rede.
[111] BARATT, Monica J.; ALDRIDGE, Judith; MADDOX, Alexia. *Op. cit*., p. 185.
[112] PERGUNTAS Frequentes Encontre as respostas para as perguntas frequentes e mitos sobre o Bitcoin. **Bitcoin.org**. Disponível em: https://bitcoin.org/pt_BR/faq#o-que-e-bitcoin. Acesso em: 13 abr. 2020.

transações, sem uma autoridade central responsável por realizar essas atividades. Em 2009, tal conceito foi publicado em uma lista de criptografia disponibilizada por Nakamoto e Malmi e, atualmente, a rede *Bitcoin* não possui um proprietário específico, mas uma rede mundial de desenvolvedores que buscam aperfeiçoá-la[113].

Shimabukuro e Silva[114] ainda explicam que as páginas que se encontram na *Dark Web* não seguem as normas da *Internet Corporation for Assigned Names and Numbers* (ICANN), entidade vinculada ao governo dos EUA que desempenha as seguintes funções: alocação do espaço de endereços do protocolo IP; atribuição dos identificadores; gerenciamento de domínios e códigos de países na Internet.

A *Dark Web* é a parte da *Deep Web* na qual se desenvolvem diversas atividades ilegais, como comércio de drogas, armas e disponibilização de conteúdo ilícito, como pornografia infantil[115]. Existe inclusive uma classificação para o conteúdo existente na *Dark Web* composta por cinco tipos. O primeiro é relativo ao entretenimento e pode incluir material devidamente regulamentado, como a pornografia adulta, ou não, no caso da pornografia infantil. O segundo é o material autorreferencial que explica aos usuários como utilizar o *Tor*. Há ainda um tipo referente ao mercado de objetos ilícitos, como armas ou drogas. Outro tipo refere-se a conteúdo sobre fraudes que podem ser cometidas pela Internet [116].

O quinto tipo de conteúdo encontrado na *Dark Web* é o mais intrigante, pois nessa categoria se encontram os serviços que estão de acordo com o propósito do *Tor*, como e-mails anônimos, fóruns e redes sociais. Trata-se de um espaço onde não há interferência ou qualquer tipo de controle e onde é possível compartilhar material que seria proibido na *Surface Web*, como textos que configuram discurso de ódio. Contudo, nem sempre os serviços disponíveis nessa categoria da *Dark Web* são utilizados para atividades ilícitas, podendo ser úteis em países onde há censura para que os usuários possam ter acesso à informação[117].

Um exemplo do uso do software *Tor* para disponibilizar informações em países nos quais o conteúdo de determinados sites foi a ação da BBC realizada em 2019. A empresa de rádio e

---

[113] *Ibidem, loc. cit.*
[114] SHIMABUKURO, Adriana; SILVA, Melissa Garcia Blagitz de Abreu e. Internet, Deep Web e Dark Web. In: SILVA, Angelo Roberto Ilha da. **Crimes Cibernéticos**. Porto Alegre: Livraria do Advogado, 2017, p. 256.
[115] PRASAD, M. R. Murali. *Op. cit*., p. 419
[116] BARATT, Monica J.; ALDRIDGE, Judith; MADDOX, Alexia. *Op. cit*., p. 186-187
[117] *Ibidem, loc. cit.*

televisão do Reino Unido disponibilizou o seu site na *Dark Web* para burlar o controle governamental que ocorre em alguns locais. A China, o Irã e o Vietnã são alguns exemplos de países que sofrem com censura por parte dos respectivos governos, que bloqueiam determinados portais de notícias como a BBC, conduta que viola o direito fundamental à informação da população[118].

Percebe-se que a *Dark Web* não é sempre utilizada para realização de atividades ilícitas, da forma que é amplamente divulgada pela imprensa e pela doutrina. Esse entendimento já está começando a ser modificado por alguns canais de comunicação, como a BBC e o jornal *The Independent*[119]. Assim como esse conceito está passando por mudanças, a noção de hacker também está começando a ser revista pela sociedade em geral, como será abordado na subseção seguinte.

2.3 CULTURA HACKER

Os conceitos de hacker e cracker são empregados com cada vez mais frequência nos meios de comunicação, embora nem sempre as informações transmitidas sobre esses conceitos sejam procedentes. Ao mencionar o Dicionário da Língua Espanhola do ano de 2018, Palazzi leciona que há duas definições para o termo hacker. Para uma delas, a palavra designa um "pirata informático". Já de acordo com o segundo conceito, o substantivo hacker refere-se a um indivíduo que possui elevada capacidade no que tange ao uso de computadores e se dedica a melhorar a segurança dos sistemas por meio do desenvolvimento de novas técnicas[120].

O termo "hacker" inicialmente era uma gíria utilizada pelos estudantes do Instituto de Tecnologia de Massachusetts entre as décadas de 1950 e 1960 para designar uma travessura mais elaborada, como cobrir uma cúpula de um dos prédios do campus com papel alumínio, conforme elucida Levy[121]. Seria algo como um projeto sem uma finalidade específica, apenas por diversão. As atividades dos hackers, de acordo com Palazzi, tiveram início com a adulteração de sistemas telefônicos com o intuito de realizar chamadas gratuitas. Posteriormente, as ações desenvolvidas por essas pessoas evoluíram para possibilitar o acesso

---

[118] BBC News launches 'dark web' Tor Mirror. **BBC**, 23 out. 2019. Disponível em: https://www.bbc.com/news/technology-50150981. Acesso em: 11 dez. 2019.
[119] MURRAY, Andrew. The dark web is not just for paedophiles, drug dealers and terrorists. The Independent, 12 dez. 2014. Disponível em: https://www.independent.co.uk/voices/comment/the-dark-web-is-not-just-for-paedophiles-drug-dealers-and-terrorists-9920667.html. Acesso em: 11 dez. 2019.
[120] PALAZZI, Pablo A. **Delitos Contra la Intimidad Informática**. Buenos Aires: Colección Derecho y Tecnología. 2019, p. 176.
[121] LEVY, Steven. *Op. cit*, p. 18.

aos *bulletin board systems*, sistemas que viabilizavam a conexão entre seus usuários, e, com o advento da Internet, todo dispositivo conectado a ela pode vir a ser acessado por hackers[122].

O Instituto de Tecnologia de Massachusetts, universidade particular estadunidense que é referência no que tange a pesquisas sobre tecnologia e engenharia, é, conforme Diaz [123], considerado o berço da cultura hacker. Apesar de não ter sido popularizada, há uma "ética hacker" que apresenta os valores filosóficos e morais a serem seguidos por pessoas que fazem parte dessa comunidade. A expressão foi cunhada pelo jornalista norte-americano Steven Levy e utilizada em seu livro "*Hackers: Heroes of The Computer Revolution*", publicada no ano de 1984, considerado como uma das primeiras obras sobre o assunto.

No referido livro, Levy realiza uma nova estruturação de princípios mencionados em outros textos sobre o assunto, como "*Computer Lib/Dream Machines*", de Theodor Holm Nelson, escrito em 1974. Nelson, também estadunidense, é um filósofo e sociólogo reconhecido como um dos pioneiros da tecnologia da informação, pois desenvolveu obras que tinham por objetivo explicar para o público leigo no que consistiam os computadores e quais eram as capacidades dessas máquinas, consideradas aparelhos de tecnologia de ponta na década de 1970[124].

As normas da ética hacker devem estar de acordo com o aperfeiçoamento dos dispositivos informáticos, promovendo o desenvolvimento da tecnologia, conforme elucida Diaz. O princípio basilar dessa ideologia é o acesso livre a informações e a produção social do conhecimento livre, a serviço de uma criação em que todos possam cooperar para desenvolver a ciência e a tecnologia[125].

A ética hacker apresenta como suas principais normas: compartilhamento; abertura; descentralização; acesso livre aos computadores; aprimoramento das máquinas; melhoria do mundo, segundo a explicação realizada por Levy no prefácio de seu livro. Para a ética hacker, todas as pessoas devem ter acesso aos computadores, bem como a qualquer outro instrumento

[122] PALAZZI, Pablo A. *Op. cit*., p. 177.
[123] DIAZ, Pedro Vidal. **Devir-Hacker: empirismo, ética e ontologia na Era Informacional**. Dissertação (Mestrado em Ciência da Informação). Escola de Comunicação da Universidade Federal do Rio de Janeiro, 2017, p. 26.
[124] NELSON, Theodore Holm. **Home Page of Ted Nelson**. Disponível em: http://ted.hyperland.com/. Acesso em: 17 ago. 2019.
[125] DIAZ, Pedro Vidal. *Op. cit*., p. 26.

que possa ensinar algo acerca do funcionamento do mundo, sendo que esse acesso deve ser total e absoluto[126].

A regra anteriormente mencionada liga-se à ideia de "faça você mesmo", pois os hackers acreditam que é possível aprender bastante com os sistemas mundiais ao compreender como eles funcionam e, dessa forma, criar instrumentos novos e mais vantajosos no que diz respeito ao uso[127]. Assim, eles são contra qualquer barreira física ou legal que os impeça de fazer isso. Essa oposição é percebida sempre que um hacker visa consertar algo que, em sua visão, apresenta defeitos ou precisa ser melhorado.

Diaz menciona como exemplo a seguinte situação: um hacker precisa enviar várias mensagens para celulares diferentes. Em vez de acessar diversas vezes a *interface web* (espaço "virtual" onde a pessoa exerce o controle sobre o aparelho) para mandar uma mensagem de cada vez, ele busca entender o funcionamento da *interface web* com o intuito de desenvolver um programa automático para agilizar a emissão de mensagens, diminuindo o tempo necessário para realizar essa tarefa. Trata-se de uma situação que demonstra a valorização da eficiência informática, que se refere a um dos princípios elementares da ética hacker: toda a informação deve ser acessada livremente[128].

Embora o "código de ética" dos hackers tenha sido exposto por Levy apenas em 1984, ele teve início na década de 1960 quando organizações e empresas começaram a controlar informações e a restringir o acesso aos seus sistemas, de acordo com Mungo e Clough[129]. Para os autores, essa conjuntura fez com que os primeiros hackers idealizassem uma revolução por meio dos computadores. Essa transformação no cenário informático teria êxito apenas quando dados de todas as pesquisas disponíveis pudessem ser acessados por qualquer indivíduo.

Pode-se considerar que o que move um hacker a desempenhar suas atividades é a curiosidade. No livro *Universidade H4ck3r*, Ulbrich e Della Valle[130] citam o seguinte discurso de um hacker ao ser detido pelas autoridades após ser acusado de tentativa de extorsão: "Meu crime é a curiosidade, é subestimar os mais poderosos mesmo quando errados. Meu crime é saber

---

[126] LEVY, Steven. ***Hackers*: Heroes of The Computer Revolution**. Nova York: Dell Publishing, 1984, p. 4.
[127] *Ibidem*, p. 32-33.
[128] DIAZ, Pedro Vidal. *Op. cit.*, p. 29.
[129] MUNGO, Paul; CLOUGH, Bryan. **Approaching zero: the extraordinary underworld of *hackers*, phreakers, virus writers, and keyboard criminals**. Nova York: Random House Inc., 1993, p. 134.
[130] ULBRICH, Henrique Cesar; DELLA VALLE, James. **Universidade H4ck3r**, 4ª ed. São Paulo: Digerati Books. 2004, p. 18.

tudo sobre todos, é ser mais esperto. Estou preso, mas por uma justa causa". Para os autores, essa declaração expressa a perspectiva de boa parte dos hackers.

No entanto, é preciso ressaltar que uma parcela expressiva da comunidade hacker defende a promoção de condutas éticas, de forma que nem todos os hackers estariam envolvidos com atividades ilegais, conforme explica Palazzi[131]. O termo está assumindo, segundo o autor, um sentido mais positivo para a sociedade em geral, pois, atualmente, há vários indivíduos no mercado da informática que se autodenominam hackers. Essas pessoas prestam serviços como verificação de falhas em sistemas de segurança de empresas, sites e organizações públicas. Em alguns casos, os "alvos dos ataques" até consideram a conduta dos hackers benéfica, pois ajuda a prevenir os problemas técnicos em seu sistema de segurança, de forma que os indivíduos que encontram essas falhas são recompensados financeiramente por isso[132].

As ações dos hackers podem acarretar vantagens não apenas para empresas e organizações, mas para a sociedade em geral. Ulbrich e Della Valle mencionam um dos maiores ataques cibernéticos já ocorridos realizado em 2002 nos Estados Unidos. O resultado da ação do hacker causou prejuízos em boa parte dos servidores do país. Essa ação, contudo, mostrou falhas nos sistemas dos servidores e, o mais relevante, revelou a extrema concentração de servidores nos Estados Unidos. Na época, 70% das mensagens que circulavam na Internet passavam por servidores ou roteadores estadunidenses. Dessa forma, a atenção dos profissionais da área voltou-se para a realização de mudanças seguindo a máxima que popularizou a Internet: a comunicação deve ser descentralizada[133].

Por conta dos danos que um ataque cibernético pode causar, a atividade dos hackers também pode ser empregada como ferramenta política, sendo essa conduta denominada de hacktivismo ou protesto social cibernético, segundo Palazzi[134]. O autor menciona ainda os debates acerca da legalidade do *hacking* (práticas desenvolvidas por hackers), pois os conhecimentos dessas pessoas podem ser utilizados tanto para aperfeiçoar medidas de segurança no âmbito da informática quanto para cometer crimes.

---

[131] PALAZZI, Pablo A. *Op. cit*. p. 177.
[132] AOS 19 anos, o argentino Santiago López fez história: é o primeiro "hacker ético" a atingir a quantia de US$ 1 milhão, o equivalente a R$ 3,8 milhões, descobrindo erros de informação. **BBC**, 05 mar. 2019. Disponível em: https://www.bbc.com/portuguese/internacional-47423964. Acesso em: 29 jan. 2020.
[133] ULBRICH, Henrique Cesar; DELLA VALLE, James. *Op. cit*., p. 20.
[134] PALAZZI, Pablo A. *Op. cit*. p. 178.

As organizações criminosas também vêm se valendo do *hacking* para desempenhar suas atividades, consoante afirma Palazzi[135]. As mais influentes organizações desse tipo possuem membros que desempenham essas atividades e, segundo o autor, já foi afirmado que a criminalidade informática consegue produzir rendimentos tão elevados quanto o tráfico de entorpecentes ou até mesmo superiores.

No âmbito da cultura hacker, os indivíduos são divididos em categorias, conforme lecionam Ulbrich e Della Valle. Dependendo do grupo hacker, essa distinção pode ser entendida como uma regra ou apenas como uma identificação informal dos membros. A classe mais baixa é a dos *newbies*, palavra que significa "novato" ou "iniciante" na língua inglesa[136]. Trata-se da pessoa que ainda possui pouco conhecimento sobre informática, mas tem a intenção de aprender cada vez mais.

Além dos *newbies* há a classe denominada *lusers*, um termo cunhado por meio da união das palavras "*looser*" (perdedor) e "*user*" (usuário), tratando-se de uma expressão de cunho pejorativo. Esses indivíduos são vítimas dos hackers com frequência, por não ter muito conhecimento sobre informática, mesmo porque não têm interesse nessa área. Tal falta de entusiasmo é que difere os *lusers* dos *newbies*[137].

Há também os *lamers*, que são os usuários de dispositivos informáticos que, apesar de não possuírem conhecimentos aprofundados sobre o tema, conseguem utilizar alguns programas ou aplicativos. Esse termo vem da palavra "*lame*", que em português significa "manco". O *lame* pode vir a desenvolver interesse por programas mais simples utilizados por hackers como o *exploit*, o *scan* e o *trojan*[138].

Já o termo *wannabe*, cuja tradução poderia ser traduzida para "aspirante" em português, pode ser usado de forma positiva ou negativa, conforme elucidam Ulbrich e Dalla Valle. Em um sentido favorável, seria a pessoa que já adquiriu uma bagagem considerável de conhecimentos e está prestes a dar mais um passo na trajetória para ser um verdadeiro hacker. Na forma pejorativa, refere-se ao indivíduo que gostaria de adentrar na comunidade, mas não possui uma base sólida sobre o tema[139].

---

[135] *Ibidem, loc. cit.*
[136] ULBRICH, Henrique Cesar; DELLA VALLE, James. *Op. cit*., p. 28.
[137] *Ibidem, loc. cit.*
[138] *Ibidem*, p. 28 – 29.
[139] *Ibidem*, p. 29.

A etapa seguinte de um *wannabe*, no sentido positivo do termo, é chamada de *larval stage* (estágio de larva ou casulo em português) e também é chamada de *spawn*[140]. Trata-se de uma pessoa que possui uma habilidade satisfatória para programar computadores, mas a experiência por ela adquirida ainda não é suficiente para considerá-la um hacker.

O termo hacker, segundo Ulbrich e Dalla Valle[141], percorreu um longo caminho até designar uma pessoa com conhecimentos aprofundados em programação de computadores. No sentido original, a palavra referia-se a carpinteiros que construíam móveis com o uso de machados (*hack* em inglês é uma onomatopeia que diz respeito ao verbo cortar). A expressão começou a ser empregada para designar pessoas que se interessavam por radioamadorismo ou por mecânica.

A palavra só começou a ser utilizada para se referir ao que se entende atualmente como hacker a partir da década de 1960. Apesar de que, inicialmente, o termo não servia somente para designar programadores de computadores com bastante experiência na área, mas para se referir a qualquer pessoa que fosse especialista em algum assunto, como mecânica de automóveis, por exemplo. Acredita-se que o significado atual do termo só foi concretizado por volta da década de 1970[142].

Ressalte-se que ainda há uma parcela considerável da população que, por influência dos veículos de comunicação, considera que hacker é um sinônimo para "criminoso digital", de acordo com Ulbrich e Dalla Valle[143]. Entretanto, a comunidade hacker possui valores éticos consolidados, que não corroboram com práticas ilegais.

Ainda que as comunidades hackers não estejam mais limitadas a um espaço físico, por conta do aprimoramento e popularização da Internet, a noção de cooperação continua bastante forte no meio hacker em geral[144]. Dessa forma, surgiu a necessidade de se estabelecer algumas normas de boas práticas hackers construídas por meio de instituições, eventos e desenvolvimento de técnicas. Esse código de ética não é único, pois apresenta regras que se confundem as normas morais práticas da produção social livre, conforme elucida Diaz[145].

---

[140] *Ibidem, loc. cit.*
[141] *Ibidem, loc. cit.*
[142] *Ibidem, loc. cit*.
[143] *Ibidem, loc. cit.*
[144] DIAZ, Pedro Vidal. *Op. cit*., p. 26.
[145] *Ibidem, loc. cit.*

Os hackers de uma vertente mais tradicional do movimento defendem que seus conhecimentos não devem ser utilizados para o mal, ainda que a concepção de bem não esteja de acordo com a lei[146]. De acordo com a obra *The New Hacker's Dictionary*[147], o termo cracker foi cunhado por volta de 1980 para se referir a indivíduos com habilidades de programação pouco significativas e que usavam-nas para danificar sistemas.

Richet[148] define os crackers como pessoas que utilizam suas habilidades para criar vírus de computador e programas maliciosos (*malwares*) e se infiltrar em sistemas com a intenção de prejudicá-los. Para o autor, o que difere um hacker de um cracker é a intenção do indivíduo. O cracker seria o autor de crimes informáticos.

Sobre a diferença entre hackers e crackers, faz-se necessário lembrar a máxima de Eric Steven Raymond[149], hacker e escritor estadunidense: "a diferença básica é esta: hackers constroem coisas, crackers as destroem". O termo hacker, conforme constata Bach[150], é compreendido em um sentido negativo, pois as pessoas entendem que se trata de um indivíduo que invade dispositivos informáticos, apaga os arquivos e demais dados e assume o controle do aparelho. Trata-se, no entanto, de um conceito estabelecido em virtude da publicidade desfavorável.

Tanto os hackers quanto os crackers possuem vasto conhecimento em sistemas operacionais e ambos utilizam essa competência para transpor as barreiras desses sistemas. Contudo, o *modus operandi* deles é bastante distinto e a mídia costuma empregar esses vocábulos como se tivessem o mesmo significado, provavelmente por não ter conhecimento ou mesmo ignorar as diferenças existentes. Para Bach, o fato de a mídia utilizar esses termos como sinônimos é o mesmo que atribuir às palavras "detetive" e "bandido" o mesmo significado[151].

Os hackers não destroem ou compartilham dados intencionalmente, mas partilham informações e deixam pistas para que os administradores possam corrigir falhas na rede. Tais pessoas visam adquirir mais conhecimentos informáticos, uma vez que são autodidatas e costumam ser estimulados por desafios. Os crackers, por outro lado, são indivíduos que usam

[146] ULBRICH, Henrique Cesar; DELLA VALLE, James. *Op. cit.*, p. 29.
[147] RAYMOND, Eric S. **The New Hacker's Dictionary**. Cambridge: Mit Press, 2000, p.22.
[148] RICHET, Jean-Loup. Free Young Hackers to Crackers. **International Journal of Technology and Human Interaction**, jun.-set. 2013, p. 54.
[149] RAYMOND, Eric Steven. **How to become a hacker**. Disponível em: http://www.catb.org/~esr/faqs/hacker-howto.html. Acesso em: 16 ago. 2019.
[150] BACH, Sirlei Lourdes. **Contribuição do Hacker para o Desenvolvimento Tecnológico da Informática**. Dissertação (Mestrado em Tecnologia da Informação). Programa de Pós-graduação em Tecnologia da Informação. Universidade Federal de Santa Catarina. 2001, p.5
[151] *Ibidem, loc. cit.*

seu saber em benefício próprio, ignorando os prejuízos que possam advir de suas condutas. Apesar de muitos realizarem esses atos somente para satisfazer interesses pessoais ao causar prejuízos a pessoas físicas e jurídicas, há crackers que fazem espionagem para organizações e empresas mediante pagamento[152].

Ulrich e Della Valle explicam que há mais de uma classe de crackers. Os *phreakers* são as pessoas que possuem conhecimentos avançados na área de telefonia, podendo colocar em prática fraudes que vão desde a realização de chamadas sem pagar até fraudes para transferir faturas telefônicas. Já o *carder* é um especialista em fraudes com cartões de crédito, normalmente casos de clonagens de cartões. Existem também os *war drivers* são os crackers que utilizam redes Wi-Fi para realização de fraudes[153].

Não se pode considerar que todos os hackers estejam envolvidos em atividades criminosas, uma vez que contribuem bastante para o desenvolvimento de sistemas de segurança informáticos. Esses indivíduos identificam vulnerabilidades na segurança dos softwares e avisam aos responsáveis, algumas vezes propondo melhorias. Ademais, os hackers viabilizam o acesso à informação, pois são responsáveis pela disponibilização de diversos materiais gratuitos na Internet[154].

Há três tipos de hackers: *white hats*; *grey hats*; *black hats*. Essa classificação é feita com base nas intenções do indivíduo que está desempenhando as atividades. Os *white hat hackers* (hackers chapéus brancos, em tradução livre para o português) são aqueles que acessam o sistema ou aparelho informático com a anuência do responsável pelo sistema ou pelo dispositivo com o intuito de descobrir falhas no sistema. Esse tipo de hacker é considerado útil para as empresas que trabalham com segurança informática, pois eles contribuem para que as organizações percebam suas deficiências. Alguns indivíduos com esses conhecimentos são inclusive contratados pelas empresas. Esses hackers também são conhecidos como *sneakers* (ocultos) e um grupo de *sneakers* é chamado de *tiger team* (equipe de tigres, em tradução livre para o português). Tratam-se de hackers que realizam um trabalho ético, sendo úteis para o desenvolvimento da tecnologia da informação[155].

---

[152] *Ibidem, loc. cit.*
[153] ULBRICH, Henrique Cesar; DELLA VALLE, James. *Op. cit.*, p. 30.
[154] BACH, Sirlei Lourdes. *Op. cit*, p. 7.
[155] MUNJAL, Meenaakshi N. **Ethical Hacking: an Impact on Society**. Disponível em: https://www.researchgate.net/publication/262726769_ETHICAL_HACKING_AN_IMPACT_ON_SOCIETY. Acesso em: 17 ago. 2019.

Há também os *black hat hackers* (hackers chapéu preto), indivíduos que exploram o sistema ou rede de computadores sem a permissão do proprietário ou pessoa responsável pelos dispositivos informáticos. A meta principal desses indivíduos é causar qualquer tipo de prejuízo ao sistema, ou seja, trata-se de pessoas que utilizam seu conhecimento para danificar o sistema identificando suas falhas. O *black hat hacker* preocupa-se apenas com seus objetivos particulares, que consistem, basicamente, em destruir o sistema e seus dispositivos de segurança. É possível considerar *black hat hacker* como um sinônimo para cracker[156].

Existe ainda um terceiro tipo de hacker denominado *grey hat* (chapéu cinza). É um indivíduo que pode usar suas habilidades para propósitos bons ou ruins. Por vezes o *grey hat* age dentro dos limites legais e, às vezes, ilegalmente. Nem sempre esses hackers atuam com más intenções, mas podem cometer crimes informáticos dependendo da situação. O *grey hat hacker* não informa ao administrador do sistema qualquer alteração ou destruição[157].

Percebe-se com as explicações mencionadas anteriormente que há certa ambivalência em algumas condutas praticadas pelos hackers. Miró Llinares[158] define a prática de *phishing* como uma tática de engenharia social e estratégia técnica para obter informações e dados de pessoas sem a anuência das mesmas. Sobre o conceito de engenharia social, o autor explica que consiste em manipulação para obter informações confidenciais, que seria a técnica denominada *spoofing*, para falsear sites ou mesmo mensagens de aplicativos para levar o indivíduo a acreditar na mensagem, facilitando o acesso aos seus dados. Um exemplo de outro recurso técnico é o *pharming*, que se configura quando o hacker direciona o indivíduo a um site falso, fazendo-o acreditar que aquela é a página da Internet verdadeira.

O *spoofing*, sendo um método relativamente simples utilizado pelos hackers, mas com potencial para causar grandes prejuízos, é uma tática para o domínio da identidade de uma pessoa física ou jurídica com intuito de obter alguma vantagem, de acordo com Miró Llinares[159]. O emprego desse método não ocorre apenas em casos de *phishing*: trata-se de uma técnica empregada em diversas situações em que o hacker tenha a intenção de obter os dados de alguma pessoa.

---

[156] *Ibidem, loc. cit.*
[157] *Ibidem, loc. cit.*
[158] MIRÓ LLINHARES, Fernando. La Respuesta Final al Ciberfraude: Especial atención a la responsabilidad de los muleros del phishing. **Revista Electrónica de Ciencia Penal y Criminología**, Granada, 2013, n. 15, p. 7.
[159] *Ibidem*, p. 18.

Trata-se de uma estratégia utilizada por hackers para falsear a identidade de uma pessoa no ambiente digital com intuito de distribuir vírus informáticos ou mesmo captar informações, como mensagens pessoais ou dados bancários[160]. No Brasil o método de *spoofing* é usado com frequência para fraudes cometidas por meio do aplicativo WhatsApp, na qual uma pessoa se apossa de uma conta alheia para enviar mensagens aos contatos da vítima solicitando dinheiro em nome dela.

Existem alguns tipos de *spoofing*. No *spoofing* de e-mail, o hacker cria uma falsa conta de correio eletrônico para falsificar a conta verdadeira de outra pessoa. Dessa forma, o hacker pode trocar mensagens com os contatos da vítima sem que elas tenham conhecimento de que não estão falando com o verdadeiro titular daquela conta. Há também o *spoofing* de identificador de chamadas, no qual o hacker realiza ligações de um chip qualquer e faz com que o número da vítima apareça no identificador de chamadas da pessoa que recebe a ligação[161].

O *spoofing* de SMS, por sua vez, consiste na ocultação de uma linha telefônica para enviar certas mensagens. A criação de uma página adulterada para ludibriar pessoas, e assim obter seus dados costuma ocorrer em sites de bancos ou lojas, é uma técnica denominada *spoofing* de site. Existe ainda o *spoofing* de IP (*Internet Protocol*, principal protocolo de comunicação da Internet), que envolve a ocultação do local de origem de certo IP para burlar sistemas e praticar crimes informáticos[162].

No *spoofing* de identificador de chamadas, o hacker consiga acessar a conta de um aplicativo de mensagens utilizado pela vítima em outro aparelho celular. Esses aplicativos costumam ter a opção de solicitar o código de acesso por meio de SMS e o hacker pode, com um aparelho imitando o identificador de chamadas de outro indivíduo, entrar em contato com o correio de voz da operadora e ter acesso ao código enviado pelo aplicativo[163]. No momento de realização dessa prática, o hacker deve verificar se o celular alheio está de fato *offline*, para que não haja suspeitas.

---

[160] ALVES, Paulo. **O que é Spoofing? Técnica foi usada para hackear Sergio Moro, diz polícia.** Disponível em: https://www.techtudo.com.br/noticias/2019/07/o-que-e-spoofing-tecnica-foi-usada-para-hackear-sergio-moro-diz-policia.ghtml. Acesso em: 23 ago. 2019.

[161] *Ibidem, loc. cit.* Disponível em: https://www.techtudo.com.br/noticias/2019/07/o-que-e-spoofing-tecnica-foi-usada-para-hackear-sergio-moro-diz-policia.ghtml. Acesso em: 23 ago. 2019.

[162] *Ibidem, loc. cit.* Disponível em: https://www.techtudo.com.br/noticias/2019/07/o-que-e-spoofing-tecnica-foi-usada-para-hackear-sergio-moro-diz-policia.ghtml. Acesso em: 23 ago. 2019.

[163] *Ibidem, loc. cit.* Disponível em: https://www.techtudo.com.br/noticias/2019/07/o-que-e-spoofing-tecnica-foi-usada-para-hackear-sergio-moro-diz-policia.ghtml. Acesso em: 23 ago. 2019.

A perspectiva de Munjal[164] é bastante realista quando a autora declara que informações confidenciais não estão seguras em nenhuma área, caso haja um hacker com conhecimentos técnicos suficientes para acessá-la. A intimidade é um dos bens jurídicos que podem vir a ser violados pela conduta dos hackers, configurando um crime. Dessa forma, na seção seguinte serão realizadas algumas explanações e considerações sobre o Direito Penal Informático.

3 DIREITO PENAL INFORMÁTICO: UMA CIÊNCIA EM CONSTRUÇÃO

Inicialmente, é preciso destacar que não há uma uniformidade a respeito da nomenclatura da matéria. Há autores, como Mirentxu Corcoy Bidasolo[165] e Gustavo Eduardo Aboso[166], que denominam esse novo ramo do Direito como Direito Penal Cibernético. Já outros, como Spencer Toth Sydow[167], denomina esse campo do conhecimento como Direito Penal Informático. Existe também o termo "Direito Digital no Âmbito Criminal" utilizado por Maues, Duarte e Cardoso[168].

Em um dos primeiros estudos brasileiros sobre esse ramo do Direito, realizado por Reis[169] na década de 1990, menciona que há oito denominações: (a) abuso de computador, sendo necessário especificar o que seria um "abuso" no ambiente informático; (b) *computer crimes*, ressaltando que o crime realizado pelo computador, mas pelo agente; (c) crimes de computação, categoria que só abrangeria os crimes informáticos próprios, cujo conceito será explicado mais adiante; (d) criminalidade mediante computadores, também um termo que só inclui os crimes da categoria retromencionada; (e) delito informático, expressão usada em países de língua espanhola, que refere-se ao objeto tutelado, mas ressalte-se que nem sempre proteção da informação é o objetivo da norma; (f) fraude informática, porém é preciso destacar que nem todos os crimes praticados com ferramentas informáticas podem ser

---

[164] MUNJAL, Meenaakshi N. *Op. cit*., p. 930.
[165] BIDASOLO, Mirentxu Corcoy. Prólogo. In: ABOSO, Gustavo Eduardo. **Derecho Penal Cibernético: La cibercriminalidade y el Derecho penal em la moderna sociedad de la información y la tecnologia de la comunicación**, Buenos Aires: Editorial B de F, 2017, p. XXI.
[166] ABOSO, Gustavo Eduardo. **Derecho Penal Cibernético: La Ciber criminalidade y el Derecho penal em la moderna sociedad de la información y la tecnologia de la comunicación**, Buenos Aires: Editorial B de F, 2017.
[167] SYDOW, Spencer Toth. *Op. cit*., p. 22.
[168] MAUES, Gustavo Brandão Koury; DUARTE, Kaique Campos; CARDOSO, Wladirson Ronny da Silva. Crimes Virtuais: Uma análise sobre a adequação penal brasileira. **Revista Científica da FASETE**, 2018.1, p. 171.
[169] REIS, Maria Helena Junqueira. **Computer Crimes**. Belo Horizonte: Del Rey, 1997, p. 24.

considerados fraudes; (g) *computerkriminalität*, termo em alemão usado para designar crimes contra computadores ou atos criminosos que utilizam computadores como ferramentas[170].

Há também no Brasil uma obra pioneira na área elaborada por Gouvêa[171], que emprega a expressão "crimes por meio da informática", por entender que, além dos computadores, outros instrumentos podem ser utilizados para prática de delitos. Vianna[172], por sua vez, admite que dois termos podem ser usados: "delitos informáticos" ou "delitos computacionais", uma vez que considera o bem jurídico a salvaguarda dos sistemas informáticos ou de computadores.

Face ao exposto, parece correto o posicionamento de Crespo[173], de acordo com o qual não há consenso quanto à denominação dos crimes relacionados com tecnologia. O próprio autor[174] utiliza um termo distinto de todas as nomenclaturas mencionadas: "crimes digitais", pois são delitos praticados por meio da informática e telemática, sendo essa expressão considerada por ele mais abrangente.

Nesse trabalho será adotada a nomenclatura proposta por Sydow[175], que utiliza a denominação "crimes informáticos" por entender que se tratam de condutas que utilizam novos instrumentos conforme a tecnologia vai avançando, não se restringindo à Internet ou aos computadores, mas também empregando métodos da robótica e nanotecnologia. Sendo a informática o campo da ciência que estuda o processamento de informações por meio de dispositivos de tratamento de dados, como computadores e smartphones, e que, cada vez mais, é desenvolvido pela sociedade pós-industrial, prefere-se empregar a denominação "crimes informáticos"[176].

Aboso[177], que utiliza em sua obra tanto o termo "Direito Penal Cibernético" quanto "Direito Penal Informático", elucida que esse ramo do Direito é uma resposta aos avanços tecnológicos ocorridos na área da comunicação que geraram um ambiente propício para o

---

[170] LUBER, Stefan. Was ist Computerkriminalität?. **Security Insider**, 14 de setembro de 2018. Disponível em: https://www.security-insider.de/was-ist-computerkriminalitaet-a-741838/. Acesso em: 07 abr. 2020.
[171] GOUVÊA, Sandra. **O Direito na Era Digital: Crimes Praticados por meio da Informática**. Rio de Janeiro: Mauad, 1997, p. 54.
[172] VIANNA, Túlio Lima. **Fundamentos de Direito Penal Informático: do acesso não autorizado a sistemas computacionais**. São Paulo: Forense, 2003, p. 9-10.
[173] CRESPO, Marcelo. *Op. cit*., 49
[174] *Ibidem*, p. 50-51
[175] SYDOW, Spencer Toth. Crimes informáticos e suas vítimas. São Paulo: Saraiva, 2015, p. 56.
[176] *Ibidem*, *loc. cit*.
[177] ABOSO, Gustavo Eduardo. *Op. cit*., p. 487.

cometimento de delitos em geral, pois os sistemas telemáticos estão presentes em praticamente todo o cotidiano de boa parte da população.

A atual complexidade da conjuntura social apresenta novos riscos, que podem ser aceitos ou mesmo diminuídos, conforme Jesus e Milagres[178]. Os autores consideram que nem toda pessoa que desempenha atividades no meio cibernético será, necessariamente, vítima de crimes, mas é preciso admitir os riscos desse ambiente. Dessa forma, caberia ao Direito tutelar os bens jurídicos das pessoas para que nesse espaço se recorra à autotutela.

O Direito Penal Informático busca estudar essa nova vertente de criminalidade e procura formas para prevenir tais delitos e como estabelecer formas de punição para os autores de tais condutas, segundo explica Sydow[179]. Este autor, assim como Jesus e Milagres[180], considera que as pessoas estão cada vez mais dependentes da informática para praticar suas atividades rotineiras, de forma que se o aprofundamento nos estudos do Direito Penal Informático se faz necessário para solucionar questões que surjam sobre o assunto.

Percebe-se que o desenvolvimento do Direito Penal em direção aos assuntos concernentes ao campo da informática é um dos resultados decorrentes do paradigma denominado "sociedade de risco", termo cunhado pelo sociólogo alemão Ulrich Beck[181]. Para esse autor, quanto mais uma sociedade produz riquezas, maior será o nível de riscos decorrentes das atividades desempenhadas por seus membros. Trata-se de um raciocínio que pode facilmente ser aplicado ao cenário atual, no qual as pessoas se veem cada vez mais dependentes do uso de dispositivos informáticos.

Em sua obra, Beck[182] ainda explica que há duas condições relacionadas à mudança do paradigma da distribuição da riqueza na sociedade de escassez para a distribuição de riscos na sociedade tardia. A primeira é a redução objetiva e o isolamento social da carência material, situação alcançada por meio do nível das forças produtivas humanas e tecnológicas, assim como o nível das garantias e normas jurídicas e do Estado Social. A segunda seria o fato de que o processo de modernização desencadeia riscos e ameaças.

---

[178] JESUS, Damásio de; MILAGRE, José Antonio. **Manual de Crimes Informáticos**. São Paulo: Editora Saraiva, 2016, p. 19.
[179] SYDOW, Spencer Toth. *Op. cit*., p. 23.
[180] JESUS, Damásio de; MILAGRE, José Antonio. *Op. cit.*, p. 19.
[181] BECK, Ulrich. **Sociedade de Risco: Rumo a outra modernidade**. São Paulo: Ed. 44, 2010, p. 23.
[182] *Ibidem, loc. cit.*

Partindo dessa tese criada por Beck, Silva Sanchéz considera que a criminalidade que utiliza meios informáticos é o melhor exemplo do estágio de complexidade social atualmente, pois se tratam de situações que geram novos riscos[183]. Assim, o autor explica que há um espaço para a expansão razoável do direito penal, mas tal processo de ampliação deveria ser balizado pelos princípios de garantia clássicos[184]. Haveria, dessa forma, duas velocidades do direito penal, de acordo com Silva Sanchez. A primeira velocidade seria representada pelo "direito penal do cárcere", no qual os princípios político-criminais e processuais clássicos seriam rigidamente aplicados. Já a segunda velocidade seria configurada por casos em que as penas seriam pecuniárias ou de privação de direitos, o que viabilizaria a flexibilização de regras e princípios. Silva Sanchez cogita que poderia existir até mesmo uma terceira velocidade do direito penal, na qual regras e princípios seriam ainda mais flexibilizados, como situações que envolvam delinquência patrimonial profissional ou terrorismo[185].

Sobre os riscos que a sociedade atual enfrenta, é possível considerá-los como um produto da atual revolução tecnológica. Castells elucida que a peculiaridade dessa revolução é o uso de conhecimentos e informações para o desenvolvimento de técnicas e dispositivos que sejam capazes de processar e difundir a informação. Para este autor, houve três fases pelas quais o uso de novas tecnologias da área da telecomunicação passou durante as décadas de 1980 e 1990. Enquanto as duas primeiras etapas foram caracterizadas pelo aprendizado mediante o uso, na terceira a tecnologia foi assimilada pelas pessoas por meio da produção. Assim, formou-se um ciclo de retroalimentação entre a introdução e o desenvolvimento de uma nova tecnologia, o que resulta em uma difusão da tecnologia de forma infinita[186].

Antes de avançar para o controle jurídico das atividades praticadas no ciberespaço, viabilizadas graças ao progresso das telecomunicações, faz-se necessário diferenciar as expressões "mídia social" e "rede social", frequentemente empregadas ao tratar de interações no ciberespaço. Embora ambas sejam referentes a meios de comunicação, a mídia social seria um termo mais apropriado para designar um canal de comunicação, um sistema que dissemina informações[187].

---

[183] SILVA SANCHEZ, Jesús María. **La Expansión del Derecho Penal: aspectos de la política criminal en las sociedades postindustriales,** 2. ed. Madri: Civitas, 2001, p. 28.
[184] *Ibidem*, p. 162.
[185] *Ibidem*, p. 163.
[186] CASTELLS, Manuel. **A Sociedade em Rede – Volume 1**, 8. ed. São Paulo: Paz e Terra, 2005, p. 68.
[187] ABUKHATER, Shaima. The Impact of the Applicability of Social Media and Social Networking Sites on Business Firms' Effectiveness and Profit Field Study: Telecommunication Sector in Jordan**. International**

Dessa forma, aplicativos de mensagens como o WhatsApp e o Telegram podem ser considerados exemplos de mídia social. Durante a pandemia do COVID-19, a Organização Mundial de Saúde criou um canal no WhatsApp para disseminar informações e tirar dúvidas sobre os sintomas causados pela contaminação do vírus[188]. No Telegram, por sua vez, além da possibilidade de criar grupos, como no WhatsApp, existe uma ferramenta denominada canal que é uma forma de disseminar conteúdo para grandes públicos, pois podem ter números ilimitados de inscritos e se dividem entre canais públicos (qualquer pessoa pode acessá-los) e privados (nos quais o administrador inclui a pessoa ou esta recebe um convite para entrar no canal)[189].

Já nas redes sociais, a comunicação exigiria um vínculo mais estreito entre as pessoas que estão trocando as mensagens e o teor dessas pode se restringir a um tópico específico[190]. Existem redes sociais voltadas para os mais diversos assuntos, como promover contatos profissionais, como o LinkedIn, para conectar acadêmicos, como o Academia.edu, e mesmo para trocar resenhas de cosméticos, como o MakeupAlley.

A complexidade que algumas dessas interações acarretam à sociedade torna-se, eventualmente, objeto de preocupação dos juristas. No Brasil, de acordo com Sydow[191], há uma parte da doutrina empenhada para estudar um Direito Penal aplicado aos crimes informáticos, porém a legislação nacional ainda não é muito avançada nesse sentido. Dessa maneira, em virtude das novidades acarretadas pelo advento dos delitos informáticos, pode-se considerar que as discussões mais aprofundadas sobre o tema ainda estão se desenvolvendo.

Para combater crimes com um nível de complexidade mais elevado, que se valem das novas tecnologias para serem cometidos, Temperini e Macedo[192] destacam que é preciso que o Estado se adapte a essas mudanças. Os autores mencionam que os trabalhos doutrinários que versam sobre a cibercriminalidade, em geral, apresentam essa conclusão acerca da

---

Journal of Managerial Studies and Research (IJMSR), Ongole, jun. 2015, v. 3, Issue 6, p. 158.

[188] OMS cria canal no WhatsApp para informar avanço e tirar dúvidas sobre coronavírus. **Folha de São Paulo**, 24 mar. 2020. Disponível em https://www1.folha.uol.com.br/equilibrioesaude/2020/03/oms-cria-canal-no-whatsapp-para-informar-avanco-e-tirar-duvidas-sobre-coronavirus.shtml. Acesso em: 23 ago. 2020.

[189] PERGUNTAS frequentes sobre canais. **Telegram**. Disponível em: https://telegram.org/faq_channels/br Acesso em: 23 ago. 2020.

[190] ABUKHATER, Shaima. *Op. cit*., p. 158.

[191] SYDOW, Spencer Toth. *Op. cit*., p. 23.

[192] TEMPERINI, Marcelo; MACEDO, Maximiliano. Nuevas Herramientas de Investigación Penal: El Agente Encubierto Digital. In: DUPUY, Daniela (Direção); KIEFER, Mariana. **Cibercrimen: Aspectos de Derecho penal y procesal penal. Cooperación Internacional. Recolección de evidencia digital. Responsabilidad de los provedores de servicios de Internet**. Buenos Aires: Editorial B de F, 2019, p. 481.

necessidade de modernização da legislação e das técnicas empregadas pelo Estado para reagir a essa nova forma de comissão de delitos.

Um dos responsáveis pela criação da Internet, o britânico Timothy John Berners-Lee[193], declarou no final de 2019 que é preciso combater o mau uso dessa rede. Para tanto, será necessária a colaboração de todos os seguimentos da sociedade. Ele afirmou que os cidadãos devem pressionar as pessoas que estão no poder para que "seus direitos digitais sejam respeitados", cabendo aos governos estabelecer leis e regulamentos adequados para alcançar esse objetivo.

Faz-se imprescindível, assim, que a legislação esteja em conformidade com as mudanças realizadas pela tecnologia, consoante ressalta Carvalho[194]. Entretanto, o autor ressalta que, em países que apresentam a lei como a principal fonte, como é a situação do Brasil, o processo legislativo costuma ser mais demorado do que o advento de novas aplicações práticas da informática e suas consequências, o que não é uma escusa para que os profissionais da área jurídica não desenvolvam alguma resposta para isso.

No Brasil, a exemplo de vários países ocidentais, entende-se que o Direito Penal deve ser o último recurso utilizado para solucionar uma situação de conflito, porém, paradoxalmente, nesse país a legislação criminal foi o primeiro instrumento ao qual se recorreu para combater os delitos informáticos[195]. A Lei nº 12.737/2012[196] alterou o Código Penal para tipificar condutas praticadas por meio de uso ou contra sistemas eletrônicos, informatizados, digitais ou similares. A Lei nº 12.735/2012[197], por sua vez, determina que os órgãos da polícia judiciária devem providenciar o aparato necessário para investigar crimes informáticos. Já o

[193] GRIFFIN, Andrew. Tim Berners-Lee: creator of the web reveals plan to stop internet turning into 'digital dystopia'. **The Independent**, 25 nov. 2019. Disponível em: https://www.independent.co.uk/life-style/gadgets-and-tech/news/tim-berners-lee-internet-web-contract-founder-facebook-google-a9216686.html. Acesso em: 04 jan. 2020.
[194] CARVALHO, Ivan Lira de. **Crimes na Internet: há como puni-los**. Jus.com.br, out. 2001. Disponível em: https://jus.com.br/artigos/2081/crimes-na-internet. Acesso em: 04 fev. 2020.
[195] JESUS, Damásio de; MILAGRE, José Antonio. *Op. cit*., p. 20.
[196] BRASIL. **Lei nº 12.737**, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.. Brasília, DF, 30 nov. de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 04 fev. 2020.
[197] BRASIL. **Lei nº 12.735**, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Brasília, DF, 30 nov. de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm. Acesso em: 04 fev. 2020.

Marco Civil da Internet[198], que determina os princípios, direitos e deveres relativos ao uso da Internet no Brasil, foi sancionado posteriormente em 2014 e, apesar de não tratar de matéria penal, é um avanço no sentido de modernizar a legislação nacional.

Dessa maneira, faz-se necessária uma nova forma de compreender a aplicabilidade do Direito em situações que configurem crimes informáticos, segundo destaca Sydow[199]. Para o autor, os operadores do direito devem se dedicar ao estudo desse ramo jurídico para que seja viável o combate a essa forma de criminalidade, bem como a elaboração e aprovação de projetos de lei adequados de forma que os questionamentos sobre a matéria sejam respondidos. Na subseção seguinte serão explanados os aspectos do Direito Penal Informático.

3.1 CARACTERÍSTICAS DO DIREITO PENAL INFORMÁTICO E DA CRIMINALIDADE INFORMÁTICA

Licks e Araújo Júnior[200] elucidam que a denominação "Direito Penal Informático" foi cunhada a partir da tradução do termo "*Criminal Information Law*" criado pelo alemão Ulrich Sieber. A obra desses autores, posterior à criação das leis que alteraram o Código Penal brasileiro para tratar de delitos informáticos e ao Marco Civil da Internet, menciona a relevância de determinar o conceito de crime informático.

Os referidos autores[201] entendem que a sociedade informatizada não apenas apresenta novos bem jurídicos, mas também atribui uma dimensão mais atual para os bens jurídicos vigentes. Sobre os objetivos do Direito Penal Informático, eles explicam que há discussões acerca do que seria a finalidade buscada por esse ramo do direito: se seria proteger o sistema informático ou se o objeto de proteção seriam as informações.

O crime informático deve ser examinado de acordo com perspectivas diversas em virtude de suas características, sendo que, para tanto, as normas aplicadas frequentemente para tipificar condutas nem sempre são suficientes[202]. Tais normas frequentemente estão respaldadas na ideia que o autor e a vítima estão próximos fisicamente no momento da ocorrência do crime,

---

[198] BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.. Brasília, DF, 23 abr. de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 04 fev. 2020.
[199] SYDOW, Spencer Toth. *Op. cit*., p. 25.
[200] LICKS, Otto Banho; ARAÚJO JÚNIOR, João Marcello. Aspectos Penais dos Crimes de Informática no Brasil. **Revista do Ministério Público**. São Paulo: Nova Fase, 1994, p. 87.
[201] *Ibidem, loc. cit.*
[202] SYDOW, Spencer Toth. *Op. cit*., p. 56.

ou seja, trata-se de uma legislação que ainda não está atualizada o bastante para combater a criminalidade praticada com o uso de dispositivos informáticos.

Contudo é preciso admitir que o Direito Penal tradicional obteve avanços consideráveis no que tange ao combate de crimes transnacionais, como o tráfico de drogas, segundo ressalta Pineda[203]. Ademais, o autor considera que a criminalidade informática ainda se apresenta como um obstáculo difícil de ser superado, em virtude das mudanças tecnológicas frequentes, se manifestando também favorável à necessidade de adaptar o Direito Penal para combater esses crimes.

Esses ajustes são de extrema relevância, pois, conforme destacam Slavomír Gálik e Sabína Gáliková Tolnaiová, o ciberespaço apresenta tamanha dimensão na vida do indivíduo que pode ser considerado uma extensão desta. As pessoas têm passado cada vez mais tempo conectadas ao ciberespaço, que antes era mais uma ferramenta para trabalhar, porém, atualmente, as possibilidades nesse ambiente são mais variadas. Nesse espaço é possível, por exemplo, estudar, realizar transações bancárias e atividades de lazer. Dessa forma, o ciberespaço pode ser entendido como uma nova dimensão existencial do indivíduo e o Direito Penal não pode se omitir frente às violações de bens jurídicos que ocorrem nesse ambiente[204].

A vulnerabilidade do ciberespaço pode ser percebida por meio do exame de algumas particularidades, de acordo com Crespo. O ciberespaço pode processar, guardar e proporcionar o intercâmbio em tempo real de elevadas quantidades de informações, tais como fotos, vídeos e áudios. Tal capacidade é viabilizada pela estrutura descentralizada e sem hierarquia própria da Internet, o que impossibilita a criação de um órgão que possa fiscalizar tamanho volume de informações[205].

Além dessa característica, o ciberespaço é acessado cotidianamente para enviar e acessar informações, de forma que as pessoas se tornam vítimas em potencial e mesmo em agentes de delitos informáticos[206]. Os próprios componentes das Tecnologias da Informação e da Comunicação são capazes de propiciar o cometimento de crimes no ciberespaço. Nesse ambiente encontram-se fóruns de discussão e redes sociais, por exemplo, estruturas nas quais é viável cometer um crime contra a honra com maior chance de repercussão.

---

[203] PINEDA, Francisco Almenar. **Ciberdelincuencia: Teoría y Práctica**. Curitiba: Juruá Editorial, 2018, p. 29.
[204] GÁLIK, Slavomí; TOLNAIOVÁ, Sabína Gáliková. *Op. cit.*, p. 5.
[205] CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Editora Saraiva, 2011, p. 46.
[206] *Ibidem, loc. cit.*

Com alguma frequência ocorrem situações nas quais as pessoas não têm noção de que podem estar cometendo crimes ao propagar suas convicções na Internet. No estado do Maranhão, o elevado número de processos envolvendo crimes contra a honra praticados em redes sociais motivou a criação da campanha denominada "*Diga o que pensa, mas sem ofender ninguém*" [207], no ano de 2018. O objetivo da ação do Ministério Público do Estado do Maranhão foi realizar a conscientização das pessoas acerca do uso adequado das redes sociais.

Percebe-se que com essa expansão do ciberespaço, novos valores surgiram, como, por exemplo, a administração das informações compartilhadas na Internet[208]. Antigamente, não era possível mensurar o valor de uma curtida em uma rede social, o pagamento de uma conta no âmbito do ciberespaço, ou a repercussão negativa de uma postagem em um blog, mesmo porque as pessoas não imaginavam que a informática possibilitaria tantas atividades nesse ambiente.

Para elucidar essas mudanças que o ciberespaço provoca no Direito Penal, Sydow recorre a conceitos da dogmática penal, como o "*malum in se*" e o "*malum prohibitum*". O primeiro termo refere-se à noção de que algumas condutas consideradas nocivas para a sociedade podem ser percebidas dessa forma por qualquer indivíduo dotado de um nível mínimo de discernimento em certa etapa da evolução social. Por exemplo, a maior parte das pessoas tem consciência de que o emprego da violência ou de grave ameaça para obter alguma vantagem é uma conduta reprovável. Assim, o *malum in se* designa o reconhecimento de ações execradas pela coletividade[209].

Já o *malum prohibitum* é a concepção de que o Direito Penal não deve somente distinguir as condutas rechaçadas pela sociedade e tipificá-las, mas também precisa averiguar quais são os bens jurídicos considerados fundamentais para que as atividades sociais prossigam, com respaldo nos valores coletivos[210]. Dessa maneira, há práticas que não são de forma absoluta condenáveis sob uma perspectiva moral, mas, por motivação política, são consideradas criminosas. Um dos casos nesse sentido é a previsão dos crimes contra a propriedade intelectual. Como todo bem jurídico é uma criação humana e a informática é uma dessas

[207] MINISTÉRIO PÚBLICO DO ESTADO DO MARANHÃO. MPMA cria campanha para alertar sociedade sobre ofensas em redes sociais. **Ministério Público do Estado do Maranhão**. 27 mar. 2018. Disponível em: https://www.mpma.mp.br/index.php/lista-de-noticias-gerais/11/14254. Acesso em: 08 fev. 2020

[208] SYDOW, Spencer Toth. El Impacto de la Informática en El Sistema Jurídico Penal Brasileiro. In: RIQUERT, Marcelo A. (direção); SUEIRO, Carlos Christian (coordenação). **Sistema penal e informático: ciberdelitos, evidencia digital, TICS**. Buenos Aires: Hammurabi, 2019, p. 286.

[209] *Ibidem, loc. cit.*

[210] *Ibidem, loc. cit.*

invenções, a violação dos novos valores por ela estabelecidos pode ser considerada uma conduta criminosa, caracterizando uma situação na qual se aplica o conceito de *malum prohibitum*[211].

Dentre as diferenças da criminalidade do "mundo real" e a criminalidade informática, Sydow[212] ressalta que a primeira apresenta padrões de mais fácil verificação, tal como identificação de locais com maior ocorrência de uma espécie de delito, o que facilita a criação de políticas públicas de prevenção, situação distinta da criminalidade informática. Essa nova criminalidade dispensa contato físico entre autor e vítima, acontece em um ambiente sem governo ou território específico, bem como inexiste um esquema específico para o cometimento de delitos informáticos.

As idiossincrasias desse ramo da criminalidade, como a dificuldade para se investigar os delitos e ausência de um padrão para o cometimento desses crimes, demandam que o Direito Penal material dos Estados sofra certas alterações por meio de reformas legislativas, conforme afirma Pineda[213]. Com a finalidade de garantir os direitos fundamentais por meio da proteção dos bens jurídicos, se faz necessária a intervenção de um Direito Penal adequado para o combate à criminalidade informática.

Outra vantagem que os crimes em meio ambiente informático apresentam em relação aos crimes do "mundo real" é a possibilidade de o autor permanecer anônimo. Segundo Aboso[214], esse aspecto proporciona mais chances de causar prejuízos ao patrimônio das vítimas, o que incentiva os criminosos a desenvolver mais técnicas que lhes permitam enganá-las e, assim, conseguir obter mais vantagens econômicas delas.

Um termo para designar o ramo do Direito que se ocupa de todas as atividades delituosas que causem prejuízo para sistemas informáticos e técnicas de telecomunicações foi elaborado pelo autor alemão Kochheim, citado por Aboso: *Kommunikationstechnik-Strafrecht* (*Iuk-Strafrecht*, em sua forma abreviada). Aboso traduz essa palavra como "Direito Penal da Informação e das Técnicas de Comunicação", disciplina que estuda todas as formas de crimes informáticos[215].

---

[211] *Ibidem*, p. 287.
[212] SYDOW, Spencer Toth. **Crimes Informáticos e Suas Vítimas**. São Paulo: Saraiva, p. 56.
[213] PINEDA, Francisco Almenar. *Op. cit.*, p. 61.
[214] ABOSO, Gustavo Eduardo. *Op. cit.*, p. 9.
[215] *Ibidem*, p. 23.

Em sentido estrito, o *Iuk-Strafrecht* trata de todas as formas de manifestação dos crimes informáticos. Ao conferir um significado mais restritivo para esse ramo do Direito, ele se volta apenas para a questão da tutela dos sistemas de processamento de dados. Essa proteção abarca não somente o dispositivo individual, mas também a técnica utilizada na rede de comunicação e a responsabilidade do administrador dessa rede. Já em sentido mais abrangente, o *Iuk-Strafrecht* inclui todas as formas de criminalidade que possam ser praticadas com o uso de sistemas de processamento e trocas de dados[216].

Além do termo *Iuk-Strafrecht*, cabe destaque a expressão *Internetkriminalität*, cunhada pelos autores alemães Malek e Popp, para designar os ataques cibernéticos propriamente ditos ou investidas contra os sistemas informáticos, considerados uma parcela da criminalidade informática. Essa forma específica de criminalidade é chamada pelos autores de *Informationsstrafrecht* ou Direito Penal da Informação, conforme a tradução de Aboso[217].

Para esse autor, uma das características do Direito Penal da Informação é ter como objeto de proteção a integridade e o funcionamento adequado dos sistemas de processamento de dados. Ademais, Aboso destaca que a conduta cometida por autores de crimes informáticos, que conseguem se manter anônimos e, mediante o uso de um computador com acesso à Internet, acessam sem autorização sistemas informáticos alheios abrange todos os componentes que formam a base dessa nova forma de criminalidade[218].

Ao partir do princípio de que há uma mudança de paradigma, Sydow[219] propõe algumas características da delinquência informática que devem ser compreendidas para definir a extensão das mudanças no Direito. São elas: a) interatividade; b) mobilidade; c) conversabilidade; d) conectividade; e) ubiquidade; f) mundialização; g) fracionabilidade; h) divisibilidade; i) intangibilidade; j) disponibilidade; k) pluralidade; l) velocidade; m) não-territorialidade.

Sobre a primeira característica, sendo a informática uma ciência que pressupõe a participação humana, Sydow[220] elucida que qualquer dispositivo informático necessita da prática de comandos para que a informação se processe. Qualquer dispositivo informático, como um

---

[216] *Ibidem, loc. cit.*
[217] *Ibidem*, p. 24.
[218] *Ibidem, loc. cit.*
[219] SYDOW, Spencer. *Op. cit.*, p. 89.
[220] *Ibidem*, p. 90-91.

tablet, um smartphone ou um notebook, por exemplo, só realizam certa atividade se forem programados por seu usuário, ou seja, dependem de uma interação para seguir um comando.

Considera-se que o entendimento acerca da interatividade como característica da delinquência informática pode passar por uma reformulação na medida que dispositivos com Inteligência Artificial sejam aperfeiçoados. Carolina Bigonha[221] define Inteligência Artificial como uma área de estudo que começou a ser desenvolvida em 1950 com o intuito de construir sistemas com desempenho semelhante ao de um ser humano quanto à resolução de problemas e aprendizado. Quando tais dispositivos atingirem um grau mais elevado de sofisticação, é possível que a noção de interatividade tenha que ser revista.

Outro aspecto que vem evoluindo cada vez mais e que favorece a delinquência informática é a mobilidade, também chamada de portabilidade[222]. Dispositivos informáticos estão se tornando cada vez menores, como, por exemplo, os já mencionados notebooks e smartphones. Ademais, a potencialização de tecnologias de satélite como *bluetooth* e tecnologias populares de acesso sem fio, como o *Wi-Fi*, viabilizam a conexão entre os aparelhos e a Internet.

Em sua obra, Manuel Castells menciona que os estudos no campo da microeletrônica tiveram início antes da década de 1940, mas que os avanços mais expressivos só ocorreram a partir da Segunda Guerra Mundial, com o advento do primeiro computador programável e do transistor, elemento considerado essencial para a microeletrônica. Outro passo decisivo para viabilizar a microeletrônica em outros dispositivos ocorreu em 1971 com o desenvolvimento do microprocessador, o computador em um único chip. Essa invenção permitiu que outros aparelhos tivessem também a capacidade de processar informações[223].

Há outra característica da criminalidade informática denominada "*talkability*", que pode ser traduzida para a língua portuguesa como a expressão "conversabilidade", conforme elucida Sydow[224]. Trata-se da capacidade dos dispositivos informáticos se comunicarem entre si, ainda que sejam de marcas distintas, viabilizando a troca de informações, fazendo com o que esses aparelhos se complementem. No Brasil já existem equipamentos com essa proposta há

[221] BIGONHA, Carolina. Inteligência Artificial em perspectiva. **Panorama Setorial.** São Paulo, ano 10, n. 2, out. 2018, p. 2.
[222] SYDOW, Spencer. *Op. cit.*, p. 89-90.
[223] CASTELLS, Manuel. *Op. cit.*, p. 77.
[224] SYDOW, Spencer. *Op. cit.*, p. 92.

alguns anos, uma aptidão que, inicialmente, foi bastante útil em especial para controlar remotamente a impressão de materiais, como documentos, por exemplo[225].

A conectividade, por sua vez, é a característica que viabiliza a conexão de um aparelho com outros, mas também com a rede[226]. A maior parte dos novos aparelhos apresentam essa capacidade com o intuito de viabilizar o acesso à Internet e para a comunicação entre dispositivos. É uma tendência que ganhou força no mercado de eletrônicos desde o ano de 2012, conforme declarou Shawn DuBravac, professor da Universidade George-Washington e, à época, diretor de pesquisa da Consumer Electronics Association, entidade que representa os fabricantes de produtos eletrônicos nos EUA, em entrevista para o jornal O Estado de São Paulo. Segundo DuBravac, a ideia é que a conectividade seja expandida para cada vez mais aparelhos além dos celulares e computadores, como, por exemplo, eletrodomésticos[227].

Um aspecto que pode ser compreendido ao analisar o aumento do índice das pessoas que têm acesso à Internet é o da mundialização[228]. O preço acessível promovido por empresas que viabilizam esse serviço, bem como a crescente oferta de ferramentas gratuitas e a expansão da capacidade de armazenamento, são fatores que atraem os internautas, de forma que é possível considerar que, atualmente, há uma geração que já nasceu conectada.

Uma reportagem veiculada no site da revista Exame menciona a obra da psicóloga Jean Twenge sobre o assunto. De acordo com a tese de Twenge, os jovens nascidos a partir de meados da década de 1990 são mais informados e tolerantes, mas, ao mesmo tempo, apresentam mais transtornos mentais e formam vínculos mais frágeis por viverem conectados à rede mundial de computadores praticamente desde o início da sua existência. Esses jovens, apesar de possuírem mais conhecimento sobre a Internet, podem, assim como o restante da população, pelo simples fato de acessarem à rede, sofrerem alguma violência nesse ambiente[229].

---

[225] IMPRESSÃO à distância é o ponto-chave das novas multifuncionais da HP. **Correio Braziliense**, 26 out. 2010. Disponível em: https://www.correiobraziliense.com.br/app/noticia/tecnologia/2010/10/26/interna_tecnologia,219997/impressao-a-distancia-e-o-ponto-chave-das-novas-multifuncionais-da-hp.shtml. Acesso em: 09 fev. 2020.
[226] SYDOW, Spencer. *Op. cit.*, p. 93.
[227] ROCHA, Camilo. Tudo Conectado: entrevista com Shawn DuBravac, economista-chefe da CEA, entidade que organiza a Consumer Eletronic Show. **O Estado de São Paulo**, 08 jan. 2012. Disponível em: https://link.estadao.com.br/noticias/geral,tudo-conectado,10000036849. Acesso em: 09 fev. 2020.
[228] SYDOW, Spencer. *Op. cit.*, p. 94.
[229] FONSECA, Joel Pinheiro da. Conectados e Solitários: a Geração Z. **Exame**, 16 dez. 2017. Disponível em: https://exame.abril.com.br/economia/conectados-e-solitarios-a-geracao-z/. Acesso em: 09 fev. 2020.

Já a fracionabilidade é um traço da delinquência informática consistente na possibilidade de sintetizar os dados em partes da programação[230]. Essa característica explica que artigos considerados economicamente relevantes consistem em longas cadeias de dados, que podem ser alteradas em todo ou em parte com a retirada, inclusão ou modificação de suas linhas de programação. Em suma, dados contidos em um ambiente informático podem ser violados por hackers, de modo que o arquivo que os continha não desempenhe sua função conforme o previsto.

O aspecto retromencionado da delinquência informática não apresenta o mesmo significado que a característica da divisibilidade[231]. A fracionabilidade diz respeito à composição dos dados e a viabilidade de separá-los em segmentos, ou seja, trata-se de um elemento inerente à programação informática. Já a divisibilidade relaciona-se à maneira de transferência desses dados para a Internet. A rede mundial de computadores é difusa, ou seja, os dados podem percorrer várias rotas até chegar ao seu destino e, para garantir que estejam na ordem correta ao final do processo de transmissão, criou-se a forma de transmissão por "pacotes".

O termo "pacote" é empregado no campo da informática para designar conjuntos de dados enviados por meio da rede[232]. São chamadas de "colisões" as perdas que ocorrem quando dois ou mais *hosts*, equipamentos utilizados para o processamento das aplicações e conexão à redes, tentam transmitir dados em sincronia empregando o mesmo meio físico. Sob o prisma jurídico, Sydow[233] destaca que é quase inviável controlar os percursos dos pacotes até chegarem ao destino, pois eles podem passar por vários países, com leis diferentes sobre temas como, por exemplo, direitos autorais ou pornografia infantil.

Faz-se necessário elucidar que a sociedade pós-industrial produziu um novo item de valor, a informação, que, conforme Sydow[234], é um bem imaterial que goza de proteção do Direito. Entretanto, a intangibilidade dos dados acarreta embaraços para a legislação existente, uma vez que, para o autor, é preciso criar uma legislação que se adeque a essa característica do bem jurídico em questão. O Brasil já está modificando suas normas para se adaptar a essa realidade com o advento da Lei Geral de Proteção de Dados[235]. Ocorre que esse aspecto dos

---

[230] SYDOW, Spencer. *Op. cit*., p. 93.
[231] *Ibidem*, p. 97.
[232] FRANCISCATTO, Roberto; CRISTO, Fernando de; PERLIN, Tiago. **Redes de Computadores**. Santa Maria: Universidade Federal de Santa Maria, 2014, p. 26.
[233] SYDOW, Spencer. *Op. cit*., p. 99-100.
[234] *Ibidem*, p. 101.
[235] BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Brasília, DF, 19 dez. 2018. Lei Geral de Proteção de Dados

dados também apresenta outro obstáculo: a vítima, por vezes, não percebe imediatamente que foi lesada ao ter seus dados acessados sem autorização.

A disponibilidade pode ser explicada como a possibilidade de acessar os dados disponíveis no próprio dispositivo informático do usuário e a opção de acessar os programas e serviços contratados de forma gratuita ou onerosa[236]. Tal característica pode constituir um fator relevante em duas situações: o computador pode ser o alvo do ataque ou mesmo um serviço utilizado por uma pessoa, como uma conta de e-mail. Essas circunstâncias podem ocasionar conflito de normas jurídicas de Estados distintos. Já existe uma iniciativa nos Estados Unidos nesse sentido denominada *Cloud Act* (Lei da Nuvem, em tradução livre para o português), legislação que propõe acordos internacionais entre Estados para solucionar situações de colisão entre leis distintas e, dessa forma, garantir o direito à privacidade e as liberdades civis dos usuários da Internet[237].

A distinção que apresenta mais destaque na comparação entre o ambiente informático e o mundo material é a composição. Na informática, os elementos são constituídos por *bits*, enquanto os objetos no espaço tangível são compostos por matéria. Todo dispositivo informático é apto para modificar dados e pode ler da mesma forma uma determinada sequência de *bits*, qualquer que seja o usuário. Dessa forma, é possível que existam arquivos idênticos em vários dispositivos informático, o que pode acarretar crimes de violação à propriedade intelectual[238].

A ciberespionagem, que consiste na invasão de sistemas informáticos para obter documentos, bem como na inserção de programas nocivos com o mesmo objetivo[239], é uma prática que causa bastantes prejuízos para esse bem jurídico em questão. Os danos financeiros anuais são estimados entre oitocentos milhões a um bilhão de dólares, em valores de direitos de propriedade intelectual[240].

Pessoais (LGPD). Brasília, DF, 14 ago. 2018. Acesso em: 09 fev. 2020

[236] SYDOW, Spencer. *Op. cit*., p. 103-104.

[237] DUPUY, Daniela; KIEFER, Mariana. La Nueva Ley "Cloud Act" su Impacto em Investigaciones en Entornos Digitales. In: RIQUERT, Marcelo A. (direção); SUEIRO, Carlos Christian (coordenação). **Sistema penal y informática: ciberdelitos, evidencia digital, TICS**. Buenos Aires: Hammurabi, 2019, p. 219.

[238] SYDOW, Spencer. *Op. cit*., p. 105.

[239] WOLOSZYN, André Luis. Ciberespionagem: Entraves na Apuração de Provas e Responsabilização no Processo Penal. In: BRASIL, Ministério Público Federal. **Crimes Cibernéticos**. Brasília: 2018, p. 138.

[240] *Ibidem*, p. 139.

Já a característica da ubiquidade, também chamada de simultaneidade, decorre da evolução da tecnologia, que possibilita que arquivos sejam trocados e que indivíduos se comuniquem há quilômetros de distância, dando a impressão de que a pessoa está no mesmo lugar que a outra[241]. Tal aspecto do ambiente informático inclusive já foi reconhecida como uma vantagem no âmbito do Processo Penal, sendo o teleinterrogatório uma prática que não viola os direitos fundamentais, desde que sejam assegurados ao réu os direitos da ciência prévia, participação efetiva e ampla defesa[242].

Contudo, ainda persistem dúvidas causadas por essa característica no âmbito do Direito Penal Informático, pois uma conduta pode ser considerada criminosa em um país e não em outro[243]. Del Carril[244] se manifesta nesse sentido ao mencionar que a Internet possibilitou que o *iter criminis* de diversos delitos possa ocorrer em múltiplas jurisdições nacionais. Esse fato levou à criminalização de algumas condutas por certos blocos de países, com o intuito de conciliar as legislações, tal como aconteceu na União Europeia[245].

Além disso, sendo a tecnologia universal, ou seja, o fato de que qualquer um pode utilizá-la, criou-se uma sensação de insegurança sobre o usuário conectado, porque o mesmo possui somente uma identidade presumida, não sendo possível ter certeza da identificação da pessoa[246]. Aboso[247] explica que o anonimato, juntamente com a falta de precaução das pessoas ao compartilhar informações privadas que podem ser utilizadas para o cometimento de crimes, são circunstâncias que favorecem a delinquência informática.

O aspecto da velocidade também apresenta bastante relevância, pois condutas criminosas, tais como invasão de dispositivo informático ou violações a direitos autorais, podem ser cometidas em frações de segundos, de acordo com Sydow[248]. O autor ainda elucida que, quanto maior a velocidade e a capacidade de armazenamento do dispositivo, podem ocorrer mais ações que causem prejuízos a bens jurídicos.

---

[241] SYDOW, Spencer. *Op. cit*., p. 107.
[242] ARAS, Vladimir. Videoconferência no Processo Penal. **Boletim Científico da Escola Superior do Ministério Público da União**. Brasília, n.15, abr./jun. 2005, p. 176.
[243] SYDOW, Spencer. *Op. cit*., p. 108.
[244] DEL CARRIL, Enrique H. Desafíos del Cibercrimen Para el Derecho Internacional. In: DUPUY, Daniela (direção); KIEFER, Mariana (Coordenação). **Cibercrimen II: Nuevas conductas penales y contravencionales; Inteligencia artificial aplicada al Derecho Penal y procesal penal; Novedosos médios probatórios para recolectar evidencia digital; Cooperación internacional y victimología**. Buenos Aires: Editorial B de F, 2018, p. 384.
[245] ABOSO, Gustavo Eduardo. *Op. cit.*, p. 43.
[246] SYDOW, Spencer. *Op. cit.*, p. 110.
[247] ABOSO, Gustavo Eduardo. *Op. cit.*, p. 33.
[248] SYDOW, Spencer. *Op. cit.*, p. 112.

Conforme mencionado, um amplo leque de condutas lesivas com as características citadas pode ser praticado no ambiente cibernético. Ademais, os crimes informáticos podem ser classificados de acordo com o bem jurídico violado, sendo próprios ou impróprios, como será explanado nas próximas subseções.

3.2 CRIMES INFORMÁTICOS PRÓPRIOS

Na subseção anterior explicou-se que, por ser um ramo do Direito Penal que ainda está em desenvolvimento, a nomenclatura acerca dos termos usados nessa área ainda não foi uniformizada. Dessa maneira, será explicado nessa parte do trabalho o conceito de "crime informático próprio" de acordo com alguns autores.

Quando as condutas são praticadas contra bens jurídicos informáticos, tais como, sistemas informatizados, de telecomunicações ou de dados, Crespo[249] considera que se trata de um crime informático próprio. Ressalte-se que o autor emprega em sua obra a expressão "crime digital", enquanto nesse trabalho utiliza-se o termo "crime informático".

Os crimes informáticos próprios, denominados por Pineda[250] de "cibercrimes puros", são aqueles caracterizados pelo uso das Tecnologias da Informação e Comunicação como meio para seu cometimento e, simultaneamente, o objeto da investida do agente. Dessa maneira, esses crimes incluem situações que configuram acessos ilícitos a sistemas informáticos alheios, assim como a danificação de dispositivos informáticos ou a utilização abusiva destes.

Outro conceito para essa classificação de crime informático próprio é proposto por Jesus e Milagre[251], para os quais tal crime estaria configurado quando o bem jurídico violado for a própria informação. A legislação em matéria penal não seria suficiente para incluir as mais diversas formas de ter acesso à informação desenvolvidas com esse objetivo. Seria necessário, assim, realizar estudos mais aprofundados no campo da informática para minimizar a questão das lacunas na legislação penal.

Uma conduta típica, antijurídica e culpável voltada para investir contra um sistema informático ou seus dados, violando a sua confidencialidade, disponibilidade ou integridade,

---

[249] CRESPO, Marcelo Xavier de Freitas. *Op. cit.*, 2011, p. 63.
[250] PINEDA, Francisco Almenar. *Op. cit.*, p. 39.
[251] JESUS, Damásio de; MILAGRE, José Antonio. *Op. cit.*, p. 52.

é, nas palavras de Sydow[252], um crime informático próprio. Dessa maneira, seriam delitos de forma vinculada.

Considerando a criminalidade informática um fenômeno inerente à sociedade da informação, Aboso[253] afirma que no Direito Penal há a distinção entre os crimes que usam dispositivos informáticos como meios, como, por exemplo, o estelionato, e os ataques contra o próprio sistema informático, sendo esses últimos os crimes informáticos em sentido próprio.

Uma pessoa que se vale de um computador para cometer uma fraude está apenas usando o dispositivo como meio, assim como poderia empregar outro instrumento para realizar essa conduta [254] . Contudo, quando esse mesmo indivíduo age de forma a prejudicar o funcionamento de um sistema, como, por exemplo, introduzindo um vírus para deixar seu desempenho mais lento, alterá-lo ou destruí-lo, está praticando um crime informático próprio, também chamado de crime informático em sentido estrito.

Ao analisar as nomenclaturas propostas por autores, é possível concluir que os crimes informáticos próprios são aqueles que têm como alvo bem jurídicos como o sistema informático, bem como os dados nele contidos. Javier Augusto de Luca[255] menciona algumas práticas que se tornaram usuais no contexto histórico atual e podem ser consideradas crimes informáticos próprios, como a modificação de arquivos e senhas para obter vantagem econômica, a inserção de vírus nos sistemas para destruir arquivos ou a instalação de programas para obter informações alheias sem a autorização de seu detentor.

As ações explanadas a seguir já estão previstas em tipos penais específicos em alguns países, tais como Espanha e Argentina, porém ainda não há previsão legislativa expressa no Brasil para criminalizar essas condutas em particular.

Exemplos de fenômenos criminosos decorrentes da evolução das telecomunicações, bem como da necessidade de criação de novos tipos penais, são mencionados por Cherñavsky, Muniagurria e Moreira[256] em um trabalho sobre as modificações na legislação argentina por

[252] SYDOW, Spencer. *Op. cit.*, p. 88.
[253] ABOSO, Gustavo Eduardo. *Op. cit.*, p. 487.
[254] *Ibidem*, p. 488.
[255] LUCA, Javier Augusto de. Delitos Informáticos, Apuntes de 2016. In: DUPUY, Daniela (Direção); KIEFER, Mariana. **Cibercrimen: Aspectos de Derecho penal y procesal penal. Cooperación Internacional. Recolección de evidencia digital. Responsabilidad de los provedores de servicios de Internet**. Buenos Aires: Editorial B de F, 2019, p. 8.
[256] CHERÑAVSKY, Nora; MUNIAGURRIA, Pablo Gris; MOREIRA, Diógenes. A diez años de la Ley de

conta da delinquência informática. Segundo os autores, já existem propostas nas Câmaras do Congresso da Nação para criminalizar fenômenos informáticos mais recentes, como o "roubo de dados pela Internet", também chamado de "roubo de identidade digital". A conduta em questão consiste em captura e uso de informações e imagens de uma pessoa, utilizados para criação de um perfil falso em redes sociais.

A utilização da Internet tem como consequência o registro dos lugares frequentados pela pessoa, dos produtos que ela consome, bem como dos assuntos que lhe chamam a atenção. Ademais, um perfil nas redes sociais possibilita que o internauta entre em contato com seus conhecidos no ambiente informático. Dessa forma, a identidade de uma pessoa no ciberespaço influencia em seus relacionamentos e sua vida profissional, de modo que é um elemento pessoal, porém se estende para um conceito de um indivíduo sobre seus interesses[257]. O uso desautorizado de identidade virtual pode causar prejuízos emocionais e patrimoniais à pessoa.

Uma das formas de acessar dados confidenciais do usuário e assim suplantar sua identidade virtual é a inserção de um *malware* ou código malicioso em um dispositivo informático. Tais códigos são instruções que, uma vez introduzidas em um dispositivo, podem danificar o sistema, violando a confidencialidade dos dados, sua disponibilidade ou mesmo sua integridade[258]. A conduta em questão desrespeita o bem jurídico da segurança telemática, causando outros prejuízos ao sistema informático e, por conseguinte, ao seu titular.

Apesar de empregados frequentemente como sinônimos, os termos *malware* e vírus não apresentam o mesmo significado. Vírus são um tipo específico de *malware* que possuem a capacidade de se replicar e se espalhar[259]. Tais códigos são elaborados de forma que seja difícil realizar sua detecção no sistema informático, conforme elucida Kiefer[260], e estão se tornando cada vez mais sofisticados para burlar os programas conhecidos como "antivírus", que também estão se aperfeiçoando. Esses programas de segurança informática protegem o

---

Delitos Informáticos. Balance y Propuestas. In: RIQUERT, Marcelo A. (direção); SUEIRO, Carlos Christian (coordenação). **Sistema penal e informática: ciberdelitos, evidencia digital, TICS**. Buenos Aires: Hammurabi, 2019, p. 153.

[257] SYDOW, Spencer. *Op. cit*., p. 118.

[258] *Ibidem*, p. 122.

[259] HENRY, Alan. The Difference Between Antivirus and Anti-Malware (and Which to Use). **Lifehacker**, 21 ago. 2013. Disponível em: https://lifehacker.com/the-difference-between-antivirus-and-anti-malware-and-1176942277. Acesso em: 16 fev. 2020.

[260] KIEFER, Mariana. Dano Informático. In: DUPUY, Daniela (Direção); KIEFER, Mariana (Coordenação). **Cibercrimen: Aspectos de Derecho penal y procesal penal. Cooperación Internacional. Recolección de evidencia digital. Responsabilidad de los provedores de servicios de Internet**. Buenos Aires: Editorial B de F, 2019, p. 321.

dispositivo de vírus e de outros tipos de *malware*, mas o termo "vírus" se popularizou, de forma que as empresas optaram por utilizar o nome "antivírus"[261]. Tais ameaças podem causar danos ao software, os componentes lógicos do sistema informático, e mesmo ao hardware, elementos físicos do sistema, sendo que o prejuízo causado depende do *malware* utilizado para o ciberataque[262].

Há também o *Rogue*, também conhecido como "falso vírus", um programa que aparenta realizar a exterminação de *malwares*, mas que, na realidade, insere códigos maliciosos no dispositivo[263]. Já o *ransomware*, cuja denominação deriva da união dos termos "*ransom*" (resgate) e *ware* (derivado da palavra software) é um programa capaz de restringir o acesso a certas partes ou arquivos do sistema, para que seja cobrado posteriormente uma quantia em troca da liberação do acesso.

A prática de *spamming* é objeto de discussão no âmbito do Direito Penal, pois o termo não se refere apenas a mensagens comerciais não solicitadas que importunam as pessoas: essas mensagens também podem conter UPM, sigla da expressão "*unsolicited pornographic messages*", mensagens pornográficas não-solicitadas, ou UEM, sigla do termo "*unsolicited electoral messages*", mensagens com conteúdo eleitoral não-solicitadas[264]. Tais mensagens podem causar constrangimentos aos seus receptores, de modo que, em países europeus, a conduta só é considerada irregular quando a pessoa que recebe não autoriza o envio das mensagens, enquanto nos Estados Unidos e no Japão é permitida até que o receptor solicite que o envio seja cessado.

Uma conduta que também é considerada crime informático próprio nos termos da legislação espanhola é o "dano informático", que consiste na destruição dos sistemas informáticos e de suas partes, sejam dados, documentos ou programas, de acordo com Barranco[265]. Para esse autor, a interpretação de tal norma deve incriminar não apenas a destruição de componentes do sistema informático, mas também a alteração de um de seus componentes de modo que prejudique o seu funcionamento.

---

[261] HENRY, Alan. *Op. cit*. Disponível em: https://lifehacker.com/the-difference-between-antivirus-and-anti-malware-and-1176942277. Acesso em: 16 fev. 2020.
[262] KIEFER, Mariana. *Op. cit*., p. 326.
[263] *Ibidem, loc. cit.*
[264] SYDOW, Spencer. *Op. cit.*, p. 131.
[265] BARRANCO, Norberto J. de la Mata. La Tutela de la Integridad y Disponibilidad de Datos y Sistemas Informáticos: el Modelo Tradicional Vinculado a uma Protección Estrictamente Patrimonisl, um Mal Referente. In: RIQUERT, Marcelo A. (direção); SUEIRO, Carlos Christian (coordenação). **Sistema penal e informática: ciberdelitos, evidencia digital, TICS**. Buenos Aires: Hammurabi, 2019, p. 38-39.

É relevante destacar uma prática denominada *scamming*, um gênero de fraude cometida no ambiente cibernético que abarca várias espécies de operações danosas. O nome vem do verbo em inglês "*to scam*", que significa enganar em português. Conforme explica Sydow[266], as fraudes cometidas por meio da Internet incluem o *phishing*, o *pharming* e outros ardis para controlar o dispositivo informático alheio, de forma que se obtenha alguma vantagem em relação ao usuário.

Nessas práticas, os delinquentes informáticos elaboram golpes para que usuários que não possuem tanta familiaridade com medidas de segurança em ambientes cibernéticos ajam em conformidade com seus objetivos[267]. Essas armadilhas são conhecidas como *honey pots* (potes de mel em português), termo em inglês utilizado para designar algo muito desejado ou popular[268]. Uma tática também utilizada nesse sentido é o" "*confidence trick*" ou "truque da confiança", situação na qual o autor da conduta e vítima mantém contato, de forma que o primeiro tenta convencer a outra pessoa a lhe fornecer dados confidenciais[269].

Dentre as modalidades de *scamming*, o *phishing*[270] é uma das estratégias mais empregadas com o objetivo de enganar a vítima para obter dados pessoais praticada por meios informáticos. Trata-se de uma técnica de engenharia social que evoluiu de forma que as informações obtidas ilegalmente podem ser dos mais diversos tipos, bem como esses dados são utilizados para fins distintos, tais como fraudes com cartões de crédito ou voltadas para estelionatos envolvendo instituições bancárias em geral.

As origens do termo "*phishing*" não são precisas, o que suscita discussões nesse sentido. Petrone, Basso e Emiliozzi[271] explicam que, para alguns, a palavra "*phishing*" decorre da expressão "*password harvesting fishing*" (colheita e pesca de informações) e outros

---

[266] SYDOW, Spencer. *Op. cit*., p. 125.
[267] *Ibidem, loc. cit.*
[268] HONEYPOT, **Collins Dictionary**, HarperCollins Publishers LLC, 2020. Disponível em: https://www.collinsdictionary.com/dictionary/english/honeypot. Acesso em: 20 out. 2020.
[269] SYDOW, Spencer. *Op. cit*., p. 125.
[270] MUNIAGURRIA, Pablo H. Gris; CHERÑAVSKY, Nora A.; MOREIRA, Diógenes A.. CHERÑAVSKY, "Phishing": Abordagem do Fenômeno desde a Prevenção e a Investigação. In: In: RIQUERT, Marcelo A. (direção); SUEIRO, Carlos Christian (coordenação). **Sistema penal e informática: ciberdelitos, evidencia digital, TICS 2**. Buenos Aires: Hammurabi, 2019, p. 117-118.
[271] PETRONE, Daniel; BASSO, Mariana; EMILIOZZI, Agustina. *Phishing Attacks*: Problemáticas de su Recepción em el Ordenamento Local y Nuevos Desafíos. In: DUPUY, Daniela (Direção); KIEFER, Mariana (Coordenação). **Cibercrimen: Aspectos de Derecho penal y procesal penal. Cooperación Internacional. Recolección de evidencia digital. Responsabilidad de los provedores de servicios de Internet**. Buenos Aires: Editorial B de F, 2019, p. 278.

consideram que é proveniente do nome "*phreaking*", prática utilizada com frequência da década de 1980 para acessar linhas telefônicas ilegalmente.

O *phising* e o *spoofing*, técnica que compõe o problema metodológico tratado nesse trabalho, são procedimentos similares, a maior distinção repousa no fato de que, no caso da primeira técnica, o hacker tem a intenção de obter vantagem financeira, enquanto o autor do *spoofing* nem sempre tem essa intenção[272].

A prática de *spoofing* pode se configurar sem que o acesso desautorizado seja explícito[273]. Coloca-se, a título de exemplo, a seguinte situação: o autor da conduta utiliza uma mensagem forjada à vítima, passando-se pela empresa proprietária do aplicativo de mensagens utilizado por ela. A vítima realiza a conduta solicitada na mensagem, como a digitação de um código em certo campo do aplicativo. Dessa forma, o autor do *spoofing* pode acessar o dispositivo informático da vítima. Ataques de *phishing* podem incluir a estratégia de *spoofing*, mas o uso de *spoofing* não necessariamente está ligado a um esquema de *phishing*.

As condutas mencionadas anteriormente são crimes informáticos próprios pois afetam bens jurídicos informáticos, tais como os sistemas informáticos e os dados dos usuários, e só podem ser praticados no ambiente cibernético. Contudo, nem todos os crimes cometidos por meio do uso de meios informáticos são próprios, conforme será explicado na subseção seguinte.

3.3 CRIMES INFORMÁTICOS IMPRÓPRIOS

Quando a conduta é típica, antijurídica, culpável e cometida por meios informáticos, mas outras ferramentas poderiam ter sido utilizadas para cometê-la, está caracterizado um delito informático impróprio[274]. Tratam-se, assim, de delitos de forma livre.

Os crimes informáticos impróprios são práticas que violam bens jurídicos que já existiam antes da popularização dos dispositivos informáticos. Tais crimes, quando cometidos por meios como a Internet acarretam uma maior repercussão, como, por exemplo, os crimes contra a honra, crimes de ameaça ou mesmo crimes previstos na legislação penal

[272] DIFFERENCE between Phishing and Spoofing. **TechDifferences**, 01 fev. 2018. Disponível em: https://techdifferences.com/difference-between-phishing-and-spoofing.html. Acesso em: 16 fev. 2020.
[273] *Ibidem, loc. cit.* Disponível em: https://techdifferences.com/difference-between-phishing-and-spoofing.html. Acesso em: 16 fev. 2020.
[274] SYDOW, Spencer. *Op. cit*., p. 88.

extravagante, como o crime de distribuição de pornografia infantil, previsto no Estatuto da Criança e do Adolescente. Como há um amplo leque de crimes que, atualmente, podem ser cometidos em ambiente cibernético, serão mencionados a seguir os que apresentam impacto mais significativo na sociedade.

Uma das condutas que pode ser considerada um crime informático impróprio e que ocorre em vários países é a pornografia de vingança. A exposição pornográfica não consentida pode ocorrer por meio de disseminação de imagens de nudez total ou parcial de uma pessoa ou em ato sexual e pode ser dar por diversos meios, tais como envio de correspondências anônimas e distribuição em cartazes e folhetos [275]. O ambiente cibernético, contudo, é utilizado preferencialmente para essa prática por viabilizar que imagens sejam distribuídas para uma quantidade maior pessoas de forma mais rápida.

Para configurar uma situação de pornografia de vingança é preciso que tenha existido um relacionamento entre o autor da conduta e a vítima, de modo que o primeiro tenha acesso a esse material íntimo, de forma consentida ou não, e tal material deve ser difundido pelo autor com a intenção de causar prejuízos à vítima[276]. A situação mencionada ocorre, na maioria das vezes, porque o autor não aceita o fim do relacionamento com o sujeito passivo do crime. Um dos primeiros casos de pornografia de vingança no Brasil foi registrado em 2006 e, segundo a própria vítima, trata-se de um crime com sequelas permanentes, uma vez que não se pode garantir que todo o material foi efetivamente retirado da Internet[277].

Devido à reiteração dessa conduta, em situações envolvendo inclusive adolescentes[278], o Poder Legislativo mobilizou-se para dar uma resposta à sociedade. Em 2018 foi sancionada uma lei para tipificar a prática nos termos do Código Penal, incluindo o art. 218-C, que prevê

---

[275] SYDOW, Spencer Toth; CASTRO, Ana Lara Camargo de. Exposição Pornográfica **Não consentida na Internet: da Pornografia de Vingança ao Lucro**. Belo Horizonte: Editora D´Plácido, 2017, p. 48.

[276] IANNELLO, Romina S.; VELTANI, J. Darío. La "Pornovenganza" en el Derecho Penal Argentino. In: DUPUY, Daniela (direção); KIEFER, Mariana (Coordenação). **Cibercrimen II: Nuevas conductas penales y contravencionales; Inteligencia artificial aplicada al Derecho Penal y procesal penal; Novedosos médios probatórios para recolectar evidencia digital; Cooperación internacional y victimología**. Buenos Aires: Editorial B de F, 2018, p. 76.

[277] NOMURA, Leandro. 'Crime na internet é ferida aberta', diz mãe sobre fotos nuas vazadas pelo ex. **Folha de São Paulo**, 21 maio 2017. Disponível em: https://www1.folha.uol.com.br/empreendedorsocial/minhahistoria/2017/05/1885458-crime-na-internet-e-ferida-aberta-diz-mae-sobre-fotos-nuas-vazadas-pelo-ex.shtml. Acesso em: 18 fev. 2020.

[278] BARRIO, Laura. Exposição de conteúdo erótico na internet vira crime contra a dignidade sexual. **Agência Universitária de Notícias da USP**, 13 fev. 2019. Disponível em: https://paineira.usp.br/aun/index.php/2019/02/13/exposicao-de-conteudo-erotico-na-internet-vira-crime-contra-a-dignidade-sexual/. Acesso em 18 fev. 2020.

o crime de divulgação de cena de estupro ou de cena de estupro de vulnerável, de cena de sexo ou de pornografia[279].

Ressalte-se que os menores de idade, por exposição contínua a estímulos do ciberespaço e pela falta de noção acerca dos perigos desse ambiente, acabam apresentando um potencial victimógeno considerável, principalmente no que tange à difusão de imagens de crianças e adolescentes com conteúdo pornográfico[280]. A pornografia infantil é uma questão que preocupa diversos países, sendo inclusive prevista na Convenção de Budapeste[281], primeiro tratado de prevenção e combate aos crimes informáticos.

A pornografia infantil é um dos fenômenos criminais que ganhou maior destaque no século XXI devido à popularização de dispositivos informáticos, segundo explica Fernández[282]. Atualmente, ferramentas da Internet são utilizadas para troca de material pornográfico envolvendo menores de idade, tais como fóruns virtuais, *webcams*, aplicativos que viabilizam o compartilhamento de fotos e vídeos e sites na *Dark Web*. Para o autor, esses meios são formas modernizadas do cometimento desse delito, antes praticado por meio da venda de revistas com esse material ou realização de apresentações exibicionistas nesse sentido.

No Brasil, a conduta é tipificada nos arts. 241 e 241-A da Lei nº 8.069/1990[283], também chamada de Estatuto da Criança e do Adolescente. No final de 2019, uma operação da Polícia Federal denominada de "Luz da Infância", com o objetivo de combater a pornografia infantil e a exploração sexual de crianças e adolescentes, cumpriu mandados de prisão em diversos

---

[279] BRASIL. **Lei nº 13.772** de 19 de dezembro de 2018. Altera a Lei nº 11.340, de 7 de agosto de 2006 (Lei Maria da Penha), e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para reconhecer que a violação da intimidade da mulher configura violência doméstica e familiar e para criminalizar o registro não autorizado de conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado. Brasília, DF, 19 dez. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13772.htm. Acesso em: 18 fev. 2020.

[280] MONTIEL, Irene; AGUSTINA, José R. Victimización Sexual de Menores A Través de las TIC. In: DUPUY, Daniela (direção); KIEFER, Mariana (Coordenação). **Cibercrimen II: Nuevas conductas penales y contravencionales; Inteligencia artificial aplicada al Derecho Penal y procesal penal; Novedosos médios probatórios para recolectar evidencia digital; Cooperación internacional y victimología**. Buenos Aires: Editorial B de F, 2018, p. 406.

[281] CONSELHO DA EUROPA. **Convenção sobre o Cibercrime**. Budapeste, 23 nov. 2001. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 17 fev. 2020.

[282] FERNÁNDEZ, David Lorenzo Morillas. Cuestiones Conflictivas en la Actual Regulación de los Delitos de Pornografia Infantil. In: GONZÁLEZ, Javier García (Coordenador). **Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual em Internet.** Valencia: Tirant Lo Blanch, 2010, p. 183.

[283] BRASIL. **Lei nº 8.069,** de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF, 13 jul. de 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 17 fev. 2020.

estados brasileiros[284]. Conforme informações concedidas pela polícia, o número de suspeitos identificados poderia ter sido maior, porém algumas companhias telefônicas e de fornecimento de Internet utilizam o mesmo endereço de IP para até 1.020 usuários, o que dificulta a detecção dos envolvidos nesses crimes.

Já são realizadas pesquisas nesse sentido para avaliar o comportamento dos jovens quando utilizam a Internet para elaborar estratégias para promover o bem-estar de crianças e adolescentes no ambiente cibernético. Além da pornografia infantil, há uma prática que tem se tornado constante nesse ambiente denominada *grooming*. Essa ação consiste na ameaça ou engano de um menor de idade para que aja em conformidade com pedidos de conotação sexual em frente a uma webcam ou aplicativos que viabilizem essa forma de comunicação, podendo ser inclusive praticado por adolescentes[285], ainda que alguns autores[286] defendam que o *grooming* só se configura quando há um adulto e um menor envolvidos na situação.

O termo decorre do verbo "*to groom*", que significa "instruir" ou "adestrar" em inglês, utilizado mais frequentemente em um contexto que envolve animais. O *grooming* pode ser enquadrado no crime de aliciamento de menores, previsto no Estatuto da Criança e do Adolescente. Há um projeto de lei na Câmara dos Deputados para aumentar a pena do crime de aliciamento de menores por meio de aplicativos de comunicação via Internet[287].

Uma situação que inclui não somente crianças e adolescentes em estabelecimentos educacionais, mas também adultos no contexto profissionais, é o *cyberbullying*. De acordo com Albiach[288], o *cyberbullying* ocorre quando um indivíduo é atormentado ou ameaçado no ciberespaço, sendo que, anteriormente, essa prática limitava-se ao ambiente de ensino. O filósofo Tomás de Aquino, por exemplo, era chamado pelos colegas, quando era estudante na

---

[284] PALMA, Gabriel; BOMFIM, Camila. Operação prende 39 em combate à pornografia infantil no Brasil e em mais 6 países. **G1**, 04 set. 2019. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/2019/09/04/operacao-combate-pornografia-infantil-no-brasil-e-em-outros-6-paises.ghtml. Acesso em: 17 fev. 2020.

[285] ALBIACH, Juan Pardo. Ciberacoso: Cyberbullying, Grooming, Redes Sociales y Otros Perigos. In: GONZÁLEZ, Javier García. **Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual em Internet.** Valencia: Tirant Lo Blanch, 2010, p. 58.

[286] GARCÍA, Hugo. El Denominado "Grooming": una Nueva Modalidad de Acoso en la Era Digital. In: In: RIQUERT, Marcelo A. (direção); SUEIRO, Carlos Christian (coord.). **Sistema penal e informática: ciberdelitos, evidencia digital, TICS 2**. Buenos Aires: Hammurabi, 2019, p. 286.

[287] BRASIL, **Projeto de Lei 2857/19**. Altera a Lei no 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para estabelecer aumento da pena ao crime de aliciamento de crianças e adolescentes pelo uso de aplicativo de comunicação via internet. Brasília, DF, 14 maio 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=43018290D54FE7EA03EF2C2B6F7DC3F2.proposicoesWebExterno2?codteor=1747399&filename=PL+2857/2019. Acesso em: 17 fev. 2020.

[288] ALBIACH, Juan Pardo. *Op. cit*., p. 56.

Universidade de Paris, de “boi mudo”, por conta de sua aparência corpulenta e personalidade introvertida[289].

Apesar de o *cyberbullying* propriamente dito não ser um crime conforme a legislação brasileira, condutas inclusas nessa prática podem ser tipificadas como injúria e difamação. De acordo com dados da empresa AVG Technologies, fabricante de softwares de segurança para dispositivos informáticos, 30% dos brasileiros já foram vítimas de *cyberbullying* nas empresas em que trabalham. Desde 2015 há uma lei instituindo o Programa de Combate à Intimidação Sistemática, destacando a modalidade cometida no ciberespaço no parágrafo único de seu art. 2º[290].

O compartilhamento de mensagens chistosas acerca das características de um indivíduo é uma prática frequente no *cyberbullying*, sendo um abuso do direito à liberdade de expressão, assim como a divulgação de boatos a respeito da reputação da vítima. Contudo, quando um boato gera consequências prejudiciais não apenas para a pessoa em questão, mas para a paz pública, configura-se uma situação de *fake news*[291].

O termo, que pode ser traduzido para a expressão “notícias falsas” em português, designa informações errôneas transmitidas com o intuito de manipular a população em geral, influenciando a tomada de decisões[292]. As *fake news* podem induzir a erro, difamar ou enaltecer pessoas ou instituições para chegar a um objetivo específico, como benefícios econômicos ou políticos.

Por conta de situações específicas que ocorreram nas eleições brasileiras de 2018, houve uma manifestação no Poder Legislativo para combater as *fake news*. Assim, foi sancionada no ano seguinte a Lei nº 13.834/2019[293], estabelecendo o crime de denunciação caluniosa para fins

---

[289] Sobre o assunto ver: NASCIMENTO, Carlos Arthur R. **Santo Tomás de Aquino: o Boi Mudo da Sicília**. São Paulo: EDUC, 2003.

[290] BRASIL. **Lei nº 13.185**, de 06 de novembro de 2015. Institui o Programa de Combate à Intimidação Sistemática (Bullying). Brasília, DF, 06 nov. 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13185.htm. Acesso em: 18 fev. 2020.

[291] PINHEIRO, Patrícia Peck Garrido. A responsabilidade no uso das mídias sociais em nossas comunidades. In: PINHEIRO, Patrícia Peck Garrido (Coordenadora). **Direito Digital Aplicado 3.0**. São Paulo: Thomson Reuters Brasil, 2018, p. 249.

[292] DE LUCA, Javier Augusto; LUZZA, Yamila Yael. “Fake News”: Cibercriminalidad y Libertad de Expresión em Internet. In: RIQUERT, Marcelo A. (direção); SUEIRO, Carlos Christian (coordenação). **Sistema penal e informática: ciberdelitos, evidencia digital, TICS**. Buenos Aires: Hammurabi, 2019, p. 53.

[293] BRASIL. **Lei nº 13.834**, de 04 de junho de 2019. Altera a Lei nº 4.737, de 15 de julho de 1965 - Código Eleitoral, para tipificar o crime de denunciação caluniosa com finalidade eleitoral. Brasília, DF, 04 jun. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13834.htm. Acesso em: 18 fev. 2020.

eleitorais. Além da divulgação de *fake news* com objetivos políticos, a disseminação de tais conteúdos, que, graças aos aplicativos de mensagens instantâneas, ocorre muito mais rapidamente, pode acarretar mortes violentas. Rumores envolvendo sequestros de crianças espalhados pelo WhatsApp levaram a casos de linchamento de pessoas inocentes em países como Índia e México[294].

Já o tráfico de drogas, tipificado no Brasil no art. 33 da Lei nº 11.343[295], trata-se de um crime cujo cometimento também foi bastante facilitado após a popularização de dispositivos com acesso à Internet. Desde o início dos anos 2000 já vinham sendo veiculadas informações nesse sentido, como uma reportagem do grupo de comunicação britânico BBC mencionando que a venda de entorpecentes estava ocorrendo em salas de bate-papo sem fiscalização[296].

Conforme mencionado anteriormente, a parte da rede mundial de computadores conhecida como *Deep Web* é constantemente utilizada para a realização de condutas ilícitas, sendo a parcela dessa camada onde essas atividades ocorrem chamada de *Dark Web*. No ano de 2013, o *Federal Bureau of Investigation* (FBI) ou Departamento Federal de Investigação, órgão policial dos Estados Unidos, identificou um gigantesco mercado de drogas nessa camada da Internet denominado *Silk Road*. O site conectava usuários e traficantes de produtos como heroína, ópio, cocaína, maconha, metanfetamina e LSD, sendo a forma de pagamentos em *bitcoins*. O *Silk Road* movimentava milhões e até hoje é considerado o mais emblemático mercado ilegal de drogas que já houve na Internet[297].

Esse modelo para comercialização de drogas é utilizado não somente em larga escala, com transações internacionais, mas também em proporções menores, inclusive no Brasil. No final de 2018, um estudante de química da Universidade Federal de Minas Gerais foi detido em Belo Horizonte por fabricar drogas e manter um site protegido por códigos para venda dos

---

[294] MARTÍNEZ, Marcos. Como as 'fake news' no WhatsApp levaram um povoado a linchar e queimar dois homens inocentes. **BBC**, 14 nov. 2018. Disponível em: https://www.bbc.com/portuguese/salasocial-46206104. Acesso em: 18 fev. 2020.

[295] BRASIL. **Lei nº 11.343**, de 23 de agosto de 2006. Institui o Sistema Nacional de Políticas Públicas sobre Drogas - Sisnad; prescreve medidas para prevenção do uso indevido, atenção e reinserção social de usuários e dependentes de drogas; estabelece normas para repressão à produção não autorizada e ao tráfico ilícito de drogas; define crimes e dá outras providências. Brasília, DF, 23 ago. 2006. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11343.htm. Acesso em: 18 fev. 2020.

[296] INTERNET facilita tráfico de drogas, diz relatório. **BBC**, 27 fev. 2002. Disponível em: https://www.bbc.com/portuguese/ciencia/020227_internetmtc1.shtml. Acesso em: 16 fev. 2020.

[297] LACERDA, Ricardo. O Portal de Drogas da Deep Web. **Superinteressante**, 17 maio 2018. Disponível em: https://super.abril.com.br/comportamento/o-portal-de-drogas-da-deep-web/. Acesso em: 16 fev. 2020.

produtos, segundo uma reportagem veiculada pelo jornal Estado de Minas Gerais[298]. Em seu depoimento à polícia, o estudante admitiu a prática das condutas, mas disse que não se considerava um traficante por não utilizar armas nem usar de violência no trato com as pessoas que adquiriam as drogas.

É possível perceber que os crimes praticados por meio da Internet, apesar de apresentarem maior repercussão do que quando praticados por outros meios, ainda são mais difíceis de serem denunciados e investigados, principalmente por conta do fator da anonimidade da delinquência informática ou pelo pouco aparato à disposição da polícia para averiguar tais condutas. Contudo, isso não é um empecilho para que os Estados se manifestem no intuito de combater a criminalidade informática por meio da tipificação de algumas condutas e estratégias de cooperação internacional nesse sentido.

4 LEGISLAÇÃO SOBRE DIREITO PENAL INFORMÁTICO

Conforme mencionado, a natureza da delinquência informática apresenta como uma de suas características a ubiquidade, também chamada de simultaneidade. Devido à evolução dos meios de comunicação, as pessoas conseguem, atualmente, praticar ações à distância, como, por exemplo, participar de audiências por videoconferência ou controlar as câmeras de uma empresa pelo celular. Entretanto, os autores de crimes informáticos valem-se desse aspecto para se beneficiarem, uma vez que uma conduta pode ser considerada crime em um país e não ser em outro.

O criminólogo Karuppannan Jaishankar[299] criou uma tese para explicar essa particularidade desse tipo de crime, denominada teoria da transação espacial para os cibercrimes[300]. Tal teoria visa explicar que o ciberespaço é um novo ambiente para o cometimento de crimes, bem como explica as causas dessa nova espécie de criminalidade.

Dentre as premissas dessa teoria está o enunciado de que pessoas com tendências criminógenas reprimidas no ambiente físico apresentam mais propensão a cometer crimes no

[298] PARANAIBA, Guilherme. Estudante de química oferecia "cardápio" de drogas e orientações pela Internet. **Estado de Minas Gerais**, 28 nov. 2018. Disponível em: https://www.em.com.br/app/noticia/gerais/2018/11/28/interna_gerais,1008758/estudante-de-quimica-oferecia-cardapio-de-drogas-pela-internet.shtml. Acesso em: 16 fev. 2020.
[299] Docente da Universidade Raksha Shakti, situada na Índia,
[300] JAISHANKAR, Karuppannan; CHANDRA, R. Rochin. **Space Transition Theory Simplified**. Disponível em: https://www.linkedin.com/pulse/space-transition-theory-simplified-r-rochin-chandra-k-k-jaishankar/. Acesso em: 19 fev. 2020.

ciberespaço, pois não cometeriam tais atos no espaço "real" devido ao receio de causar prejuízos à sua reputação[301]. Ademais, o conflito entre normas e valores inerentes ao espaço físico e as regras e princípios do ciberespaço favorecem a comissão de crimes informáticos, como se tem realçado. O ambiente cibernético permite que os delinquentes se movam de um local para o outro nesse espaço, graças à Internet, e possibilita que escondam sua atual localização física.

Devido a essa dinâmica apresentada pelo ciberespaço, mapear os crimes informáticos torna-se uma tarefa bastante difícil[302]. A delinquência informática logrou êxito quanto à diminuição das distâncias físicas nesse ambiente, trata-se de um fato inegável. Dessa forma, é preciso que os países atuem em conjunto para combater a criminalidade informática, porém nem todos apresentam o mesmo nível de desenvolvimento econômico necessário para lidar com essas questões, de forma que as legislações sobre o assunto não são uniformes.

A cooperação internacional se faz imprescindível para diminuir os prejuízos causados por essa nova forma de expressão delitiva comum à sociedade da informação[303]. Ademais, as organizações privadas devem participar do combate à criminalidade informática, fornecendo dados, sempre que possível, a fim de colaborar com as autoridades públicas, mesmo porque a viabilidade do controle de dados transmitidos pela Internet depende da atuação das empresas prestadoras desse serviço.

Alguns Estados mais desenvolvidos economicamente introduziram em suas respectivas legislações normas sobre crimes informáticos no início da década de 1970[304]. As medidas legais estabelecidas nessa época eram caracterizadas por previsões fragmentadas sobre a proteção de dados e estavam concentradas somente em locais onde uma parcela considerável da população já tinha acesso a computadores. Dentre os países que criaram leis nesse sentido estavam a Suécia (1973) os Estados Unidos (1974) e Alemanha (1977)[305].

---

[301] *Ibidem, loc. cit.* Disponível em: https://www.linkedin.com/pulse/space-transition-theory-simplified-r-rochin-chandra-k-k-jaishankar/. Acesso em: 19 fev. 2020.
[302] *Ibidem, loc. cit.* Disponível em: https://www.linkedin.com/pulse/space-transition-theory-simplified-r-rochin-chandra-k-k-jaishankar/. Acesso em: 19 fev. 2020.
[303] ABOSO, Gustavo Eduardo. *Op. cit.*, p. 58.
[304] LI, Johannes Xingan. Cyber Crime and Legal Countermeasures: A Historical Analysis. **International Journal of Criminal Justice Sciences**. Ahmedabad, 2017, v. 12, p. 201.
[305] SAIN, Gustavo. La Estrategia Gubernamental frente al Cibercrimen: la importância de las políticas preventivas más allá de la solución penal. In: PARADA, Ricardo Antonio (comp.). **Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet.** Buenos Aires: Erreius, 2018, p. 13.

A legislação sobre a matéria era escassa e apenas poucos países apresentavam leis nesse sentido, mas na década de 1980 outros países, especialmente os europeus, influenciados pela iniciativa dos Estados Unidos criaram normas para proteger sistemas de pagamento informáticos[306]. Leis criadas em 1970 foram alteradas para evitar a reprodução e a venda de obras digitais e países como Estados Unidos, Suécia e Japão elaboraram legislações específicas para salvaguardar as informações guardadas em chips. Durante a década de 1990, foram estabelecidas leis para definir a responsabilidade dos provedores de acesso à Internet acerca do material publicado na Grã-Bretanha, Estados Unidos e Alemanha.

Uma das questões acerca do crime informático que mais afligia (e ainda aflige) a comunidade internacional é o fato de o delito estar sujeito à jurisdições distintas, chegando a causar inclusive conflitos entre Estados, por conta do princípio da soberania, conforme destacado pela Organização das Nações Unidas[307]. Propôs-se então que as autoridades nacionais atuassem norteadas por princípios de cooperação internacional, sendo tais mecanismos imprescindíveis para combater a criminalidade informática.

Um estudo realizado para a União Europeia a respeito da questão dos crimes informáticos, no ano de 1998, revelou que os países reagiam a tais condutas conforme a legislação penal nacional, excluindo medidas de proteção alternativas[308]. Ademais, embora destacados os esforços de organizações nacionais e internacionais, as legislações dos países europeus ainda apresentam deficiências quanto às ações que envolvem *hacking*, invasão de privacidade, informações confidenciais de organizações e conteúdos ilegais. As respectivas legislações também não eram precisas quanto ao alcance da jurisdição em matéria penal no caso de crimes informáticos.

Em relação ao combate a essa criminalidade nos níveis internacional e supranacional, o estudo em questão menciona que as organizações, como a própria União Europeia, a Organização das Nações Unidas e a *International Criminal Police Organization* (Interpol), por exemplo, devem executar atividades em conjunto para alcançar tal propósito. As iniciativas nesse sentido ainda precisariam alcançar certo grau de harmonização para enfrentar os problemas decorrentes da criminalidade informática. Além disso, a maioria das respostas

[306] *Ibidem, loc. cit.*
[307] ABOSO, Gustavo Eduardo. *Op. cit.*, p. 42
[308] SIEBER, Ulrich. **Legal Aspects of Computer-Related Crime in the Information Society**, 01 jan. 1998. Disponível em: https://ec.europa.eu/archives/ISPO/legal/en/comcrime/sieber.html. Acesso em: 20 fev. 2020.

concedidas por tais organizações transnacionais seriam vagas e concentradas somente em aspectos legais[309].

O obstáculo mais comum frente à investigação de tais crimes repousa no fato de que a legislação penal sobre a matéria não é uniforme a nível global. Como exemplo é possível mencionar o caso do ataque cibernético realizado por meio do vírus *Love Bug*, realizado no ano 2000. O vírus em questão foi disseminado a partir das Filipinas, mas, como o país não possuía uma legislação que dispusesse sobre a tipificação do ato de espalhar um vírus de computador, os autores da conduta não puderam ser processados[310].

Além de tratados, há iniciativas de particulares no sentido de promover a cooperação de países, organizações e pessoas na manutenção de um ambiente informático mais sadio. Tim Berners-Lee, criador do sistema *WWW*, é responsável pela idealização do plano global denominado *Contract for the Web*[311]. Trata-se de um documento elaborado com diretrizes para governos, empresas e cidadãos para garantir a segurança do ciberespaço e promover medidas para aumentar o acesso mundial à Internet.

Para cada um dos agentes sociais que a campanha visa atingir há três diretrizes que se desdobram em mais orientações. Os três princípios voltados para os governos seriam: assegurar que todas as pessoas possam se conectar à Internet; manter a Internet disponível continuadamente; respeitar e proteger os direitos fundamentais à privacidade *online* e aos dados disponibilizados nesse ambiente[312]. O último princípio é especificamente interessante para responder à questão metodológica desse trabalho, de forma que os detalhes previstos no documento sobre essa diretriz serão analisados.

A salvaguarda do direito à privacidade e a proteção de dados são consideradas as bases para que todos possam acessar a Internet de maneira livre, segura e sem receio[313]. As medidas a serem adotadas pelos governos nesse sentido devem incluir o estabelecimento de políticas voltadas para os setores público e privado. As campanhas devem ser aplicadas a todos os

[309] *Ibidem, loc. cit.* Disponível em: https://ec.europa.eu/archives/ISPO/legal/en/comcrime/sieber.html. Acesso em: 20 fev. 2020.
[310] ABOSO, Gustavo Eduardo. *Op. cit.*, p. 43.
[311] CONTRACT FOR THE WEB. **A global plan of action to make our online world safe and empowering for everyone**. Disponível em: https://contractfortheweb.org/. Acesso em: 12 mar. 2020.
[312] ABOSO, Gustavo Eduardo. *Op. cit.*, p. 5.
[313] *Ibidem, loc. cit.*

dados, sendo irrelevante se essas informações são fornecidas pelo usuário, observadas ou inferidas.

Ademais, caso exista alguma demanda para que enseje o acesso a comunicações e dados particulares por parte das autoridades governamentais, isso deve ser feito de maneira proporcional e em conformidade com as normas internacionais de direitos humanos[314]. Os agentes públicos também não podem exigir que prestadores de serviços ou processadores de dados comprometam a segurança de seus produtos ou serviços para disponibilizar informações, de forma que tais empresas devem colaborar dentro de suas possibilidades.

Já houve situações caracterizadas por um impasse entre empresas fornecedoras de serviços nesse sentido e uma autoridade judiciária. A primeira ocorreu em 2015, quando o juiz da Central de Inquéritos da Comarca de Teresina determinou que empresas de telefonia paralisassem o acesso ao WhatsApp temporariamente em todo o país[315]. A medida foi tomada em razão da recusa da empresa responsável pelo aplicativo de disponibilizar informações para uma investigação. Contudo, o aplicativo não chegou a ficar suspenso, pois um desembargador do Piauí impediu que essa determinação fosse adiante, alegando que as empresas telefônicas e seus usuários fossem prejudicados por uma decisão judicial[316].

Pelo mesmo motivo, o juiz da 1ª Vara Criminal de São Bernardo do Campo decidiu, também no ano de 2015, suspender o funcionamento do aplicativo[317]. Como a empresa não atendeu a uma determinação judicial, o Ministério Público determinou que o WhatsApp ficasse 48 horas fora do ar. Após ficar 14 sem funcionamento, uma liminar do Tribunal de Justiça de São Paulo normalizou o acesso ao aplicativo[318].

No ano seguinte, um juiz de Sergipe proferiu uma decisão bloqueando o WhatsApp por 72 horas até que o Facebook, empresa responsável pelo aplicativo, colaborasse com uma

---

[314] *Ibidem*, *loc. cit.*
[315] DECISÃO de juiz do Piauí manda tirar WhatsApp do ar em todo o Brasil. **G1**, Teresina, 25 fev. 2015. Disponível em: http://g1.globo.com/pi/piaui/noticia/2015/02/decisao-de-juiz-do-piaui-manda-tirar-whatsapp-do-ar-em-todo-o-brasil.html. Acesso em: 12 mar. 2020.
[316] WHATSAPP bloqueado: Relembre todos os casos de suspensão do app. **G1**, São Paulo, 19 jul. 2016. Disponível em: http://g1.globo.com/tecnologia/noticia/2016/07/whatsapp-bloqueado-relembre-todos-os-casos-de-suspensao-do-app.html. Acesso em: 12 mar. 2020.
[317] WHATSAPP bloqueado: operadoras são intimadas a barrar app no país por 48h. **G1**, São Paulo, 16 dez. 2015. Disponível em: http://g1.globo.com/tecnologia/noticia/2015/12/operadoras-sao-intimadas-bloquear-whatsapp-no-brasil-por-48-horas.html. . Acesso em: 12 mar. 2020.
[318] WHATSAPP bloqueado: Relembre todos os casos de suspensão do app. *Op. cit*. Disponível em: http://g1.globo.com/tecnologia/noticia/2016/07/whatsapp-bloqueado-relembre-todos-os-casos-de-suspensao-do-app.html. Acesso em: 12 mar. 2020.

investigação criminal. Nessa situação, o WhatsApp ficou temporariamente sem funcionar por cerca de 24 horas, até que o pedido de reconsideração realizado pelos os advogados da empresa foi acolhido por um desembargador do tribunal de justiça do estado.

A quarta e, até o momento, última vez que a justiça determinou a suspensão do funcionamento do aplicativo aconteceu em julho de 2016. Uma delegacia da Polícia Civil de Duque de Caxias, município situado no Rio de Janeiro, solicitou que a empresa Facebook, responsável pelo aplicativo WhatsApp, disponibilizasse dados para uma investigação[319].

Nessa situação, a juíza responsável pela decisão que impediu os usuários de terem acesso ao aplicativo declarou que o grupo Facebook recebeu notificações para interceptar mensagens que seriam utilizadas em uma investigação em Duque de Caxias[320]. Como resposta, a empresa enviou perguntas em inglês e solicitou que as respostas fossem redigidas no mesmo idioma, desagradando, assim, a magistrada, que considerou o fato um desrespeito à língua oficial do Brasil[321]. Ademais, o Facebook solicitou informações de uma investigação realizada sob sigilo, a qual a nem mesmo a juíza possuía acesso.

Como motivo para não cumprir a ordem judicial, a empresa alegou que as mensagens trocadas pelo aplicativo são criptografadas, de forma que elas se tornam inacessíveis, assegurando o sigilo das conversas dos usuários[322]. De forma simplificada, isso significa que as mensagens são codificadas com chaves de segurança que "embaralham" os dados e, por isso, nem mesmo o próprio Facebook teria a capacidade de acessá-las.

A magistrada contra-argumentou que o Facebook não precisava quebrar a criptografia do aplicativo, mas encontrar uma solução que possibilitasse apenas a obtenção das conversas dos suspeitos[323]. Esse conjunto de princípios e técnicas, denominado criptografia, é utilizado para proteger dados sigilosos de invasões e ativistas digitais da vigilância de certos governos.

---

[319] BRASIL. Juiza quer desabilitar criptografia de suspeitos no Whatsapp; entenda. **Empresa Brasileira de Comunicação**, 19 jul. 2016. Disponível em: http://www.ebc.com.br/tecnologia/2016/07/juiza-quer-desabilitar-criptografia-no-whatsapp-entenda. Acesso em: 13 mar. 2020.

[320] WHATSAPP bloqueado: Relembre todos os casos de suspensão do app. *Op. cit*. Disponível em: http://g1.globo.com/tecnologia/noticia/2016/07/whatsapp-bloqueado-relembre-todos-os-casos-de-suspensao-do-app.html. Acesso em: 13 mar. 2020.

[321] JUÍZA diz que Facebook trata autoridade judicial 'com deszelo'. **G1**, 19 jul. 2016. Disponível em: http://g1.globo.com/tecnologia/noticia/2016/07/whatsapp-veja-perguntas-em-ingles-que-o-facebook-enviou-justica.html. Acesso em: 13 mar. 2020.

[322] BRASIL. Juiza quer desabilitar criptografia de suspeitos no Whatsapp; entenda. *Op. cit*. Disponível em: http://www.ebc.com.br/tecnologia/2016/07/juiza-quer-desabilitar-criptografia-no-whatsapp-entenda Acesso em: 13 mar. 2020.

[323] *Ibidem, loc. cit.* Disponível em: http://www.ebc.com.br/tecnologia/2016/07/juiza-quer-desabilitar-criptografia-no-whatsapp-entenda Acesso em: 13 mar. 2020.

Contudo, a criptografia também pode ser utilizada para outros fins, inclusive para acobertar o cometimento de crimes.

Percebe-se que há um impasse: a justiça brasileira exigiu que as conversas realizadas por meio do aplicativo fossem disponibilizadas, mas a empresa responsável pelo serviço declarou ser impossível abrir uma exceção para as mensagens trocadas pelos suspeitos por conta da técnica utilizada para proteger o sigilo dos usuários.

Uma das medidas previstas no *Contract for the Web*[324] para os governos dos Estados, no que tange à salvaguarda do direito à privacidade no ambiente cibernético, é efetuar somente a coleta de dados que for necessária para alcançar certo interesse público. Ademais, as autoridades estatais devem fiscalizar as organizações públicas e privadas para que cumpram a legislação concernente à matéria.

O Brasil é um dos países que não possui legislação específica para solucionar esse tipo de situação, ou seja, quando não é viável que a empresa disponibilize as informações solicitadas pela justiça. Tal fato demonstra que o legislador ainda precisa se aprofundar no assunto a fim de proporcionar respostas para essas novas demandas

Ressalte-se, entretanto, que há uma previsão nesse sentido na Convenção de Budapeste. O art. 6º do tratado dispõe sobre a utilização imprópria de dispositivos. Vejamos:

> Artigo 6º - Uso abusivo de dispositivos
> 1. Cada Parte adoptará as medidas legislativas e outras que se revelem necessárias para estabelecer como infracções penais, em conformidade com o seu direito interno, quando cometidas intencional e ilegitimamente:
> (...)
> 2. O presente artigo não deve ser interpretado como impondo responsabilidade criminal quando a produção, a venda, a aquisição para utilização, a importação, a distribuição, ou outra forma de disponibilização ou posse, mencionadas no n.º1 do presente artigo não tenham por objectivo cometer uma infracção estabelecida em conformidade com os artigos 2º a 5º da presente Convenção, como é o caso de ensaios autorizados ou de protecção de um sistema informático.

Caso o Brasil participasse da Convenção de Budapeste, seria possível invocar essa norma para solucionar a situação do conflito entre o WhatsApp e as autoridades judiciais, mas o Brasil, até o momento, não assinou o tratado. Nos tópicos seguintes serão abordadas legislações supranacionais com o intuito de combater a criminalidade informática, legislações de alguns

[324] CONTRACT FOR THE WEB. *Op. cit*. Disponível em: https://contractfortheweb.org/. Acesso em 12 mar. 2020.

Estados no combate à essa forma de criminalidade, bem como as leis brasileiras existentes com o mesmo objetivo.

4.1 LEGISLAÇÕES SUPRANACIONAIS

O advento da sociedade da informação não apresentou como consequência somente a identificação do *iter criminis* percorrido pelos crimes informáticos, que pode ocorrer em diversas jurisdições, mas também no aspecto investigatório, especificamente quanto à obtenção de provas úteis e válidas para o processo[325]. Para superar eventuais obstáculos e atingir esse objetivo, os instrumentos de assistência internacional recomendam que a cooperação entre os Estados seja o mais ampla possível, bem como uma "autoridade central" responsável por gerir tais solicitações de auxílio.

Apesar dessa questão ter se tornado objeto de atenção de vários Estados mais recentemente, a comunidade internacional vem apresentando iniciativas para suprimir os delitos informáticos desde a década de 1970. A Interpol realizou uma conferência internacional em 1979 para tratar do assunto, ressaltando que o desenvolvimento no campo das comunicações demandava um maior cuidado das organizações internacionais em relação à criminalidade informática[326].

Três anos mais tarde, a Organização para a Cooperação e Desenvolvimento e Econômico (OCDE) reuniu especialistas no assunto para adaptar a legislação penal dos Estados pertencentes a esse bloco com o objetivo de evitar o uso indevido das redes e dispositivos informáticos[327]. Em 1986, a OCDE publicou um documento denominado *Computer Related Crime: analysis of the legal policy* (Criminalidade Informática: análise da política legislativa) contendo uma lista de alguns crimes informáticos mais frequentes, para que os Estados atualizassem suas respectivas legislações.

No final da década de 1980, o Conselho da Europa divulgou algumas orientações dirigidas aos parlamentos dos países vinculados a esse órgão para prevenção de crimes cometidos por meio de dispositivos informáticos[328]. O responsável pela elaboração de tal documento foi um grupo denominado Comitê de Especialistas sobre Delitos Relacionados com o Emprego de Computadores, que abordou temas como prevenção de riscos e procedimentos investigativos.

---

[325] DEL CARRIL, Enrique H. *Op. cit*., p. 384.
[326] SAIN, Gustavo. *Op. cit*., p. 13.
[327] *Ibidem*, p. 14.
[328] *Ibidem, loc. cit*.

A Comissão da Comunidade Europeia, por sua vez, chegou a elaborar dois informes sobre a matéria, sendo um deles veiculado em 1996 e outro no ano 2000[329]. O primeiro documento abordou os desafios causados pelos ataques cibernéticos, que eram uma novidade à época, enquanto o segundo analisava a expansão da telefonia celular e suas consequências. Ademais, a Comissão tratou de assuntos como o uso de redes telemáticas para disseminação de material pornográfico infantil e com objetivos terroristas.

É possível considerar a Convenção sobre o Cibercrime[330], também conhecida como Convenção de Budapeste, assim como a Diretiva 2005/222/JHA, uma resposta normativa do Conselho Europeu ao fenômeno crescente da criminalidade informática[331]. Outras diretivas foram adotadas posteriormente no mesmo sentido, como a Diretiva 2001/413/JI, que versa sobre delitos patrimoniais, a Diretiva 2004/68/JI, sobre o combate à pornografia infantil, e a Diretiva 2008/913/JI, que trata de manifestações de violência e ódio no ambiente cibernético.

O tratado em questão versa sobre matérias de direito penal material e processual e medidas de cooperação internacional nesse sentido. De acordo com Ferreyra[332], um dos aspectos que mais despertam interesse é a análise da adaptação da Convenção sobre o Cibercrime às legislações dos Estados signatários reguladoras do processo penal e das técnicas de investigação e prevenção criminais. A Convenção apresenta várias diligências que devem ser realizadas pelos Estados partes, como o registro e confisco de dados, a obtenção de dados em tempo real ou interceptação de dados de conteúdo aparentemente ilícito.

A Convenção de Budapeste institui o princípio da colaboração entre os Estados signatários a partir de autoridades centrais, assim como uma rede disponível 24 horas em todos os dias da semana para que as pessoas que queiram denunciar crimes informáticos[333]. A constituição de uma rede nesses moldes nos Estados partes, apesar de contribuir para a identificação desses crimes e simplificar os problemas da autoridade central, não soluciona a dificuldade relacionada com o volume de informações requeridas a cada Estado por conta da expansão da interconectividade.

---

[329] ABOSO, Gustavo Eduardo. *Op. cit.*, p. 44-45.
[330] CONSELHO DA EUROPA. **Convenção sobre o Cibercrime**. Budapeste, 23 nov. 2001. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 21 fev. 2020.
[331] ABOSO, Gustavo Eduardo. *Op. cit.*, p. 45.
[332] FERREYRA, Eduardo. Una visión desde los derechos humanos sobre las tecnologias de vigilância e investigación. In: RIQUERT, Marcelo A. (direção); SUEIRO, Carlos Christian (coordenação). **Sistema penal e informática: ciberdelitos, evidencia digital, TICS.** Buenos Aires: Hammurabi, 2019, p. 114.
[333] DEL CARRIL, Enrique H. *Op. cit.*, p. 384.

Com a adoção de tais medidas, a capacidade do Estado de fiscalização é ampliada em virtude dos mecanismos tecnológicos disponíveis para alcançar esse objetivo[334]. Assim, aborda-se o seguinte dilema: é necessário conciliar a vigilância exercida pelo poder público, bem como as atividades de investigação, com a observância dos direitos fundamentais dos indivíduos. Os Estados devem tomar providências nesse sentido para harmonizar ambas as demandas.

Apesar de ter sido criado em 2001, o referido tratado entrou em vigor somente em julho de 2004. De acordo com o site[335] do Conselho da Europa, a Convenção de Budapeste é um tratado aberto não apenas para membros desse grupo, mas também para Estados que não pertencem ao Conselho. Até o último acesso ao site do Conselho da Europa havia sessenta e quatro ratificações. Dos países europeus que ratificaram o tratado, é possível mencionar a Alemanha, a França, o Reino Unido, a Noruega e a Dinamarca. Já dentre os países que não fazem parte desse grupo há a Austrália, o Canadá, os Estados Unidos e o Japão, por exemplo. O Brasil não é signatário da Convenção de Budapeste, apesar de já ter sido convidado pelo Conselho da Europa para participar da mesma[336].

Na elaboração do referido tratado, buscou-se proteger dados pessoais armazenados em bases de dados de organizações públicas e privadas, que apresentam uma dimensão tão elevada que podem ser utilizados para diversos fins[337]. Os dados podem ser empregados em questões de segurança pública e defesa estatal e até mesmo para avaliar os riscos em hipóteses de concessão de serviços como, por exemplo, atividades bancárias.

A Convenção de Budapeste especifica os conceitos de "sistema informático" e de "dados pessoais" em seu primeiro artigo:

> Artigo 1º - Definições para os fins da presente Convenção:
> a) "Sistema informático" significa qualquer dispositivo isolado ou grupo de dispositivos relacionados ou interligados, em que um ou mais de entre eles, desenvolve, em execução de um programa, o tratamento automatizado dos dados;
> b) "Dados informáticos" significa qualquer representação de factos, de informações ou de conceitos sob uma forma susceptível de processamento num sistema de computadores, incluindo um programa, apto a fazer um sistema informático executar uma função;

[334] *Ibidem, loc. cit.*
[335] COUNCIL OF EUROPE. **Chart of signatures and ratifications of Treaty - Convention on Cybercrime**. Disponível em: https://www.coe.int/en/web/conventions/full-list/ /conventions/treaty/185/signatures?p_auth=exhG7iJ7. Acesso em: 23 fev. 2020.
[336] BRASIL. Conselho da Europa convida o Brasil para compor a Convenção de Budapeste sobre o Cibercrime. **Ministério Público Federal**, 13 dez. 2019. Disponível em: http://www.mpf.mp.br/pgr/noticias-pgr/conselho-da-europa-convida-o-brasil-para-compor-a-convencao-de-budapeste-sobre-o-cibercrime. Acesso em: 23 fev. 2020.
[337] ABOSO, Gustavo Eduardo. *Op. cit*., p. 59.

Considera-se que explicação de tais termos no texto normativo é um aspecto de extrema relevância para que não haja violação ao princípio da legalidade. Na legislação brasileira que versa sobre a tipificação criminal de delitos informáticos[338], por exemplo, não há definição do que seria "dispositivo informático" ou "mecanismo de segurança". Isso pode causar alguma insegurança jurídica quanto à compreensão do assunto.

As medidas indicadas pelo Conselho de Budapeste e por outros organismos internacionais, entretanto, ainda não são suficientemente efetivas para combater a delinquência informática frente aos resultados atuais, de acordo com Sain[339]. Isso se deve ao fato de que ainda não há um consenso sobre quais condutas praticadas no ambiente cibernético poderiam ser consideradas crimes, uma vez que cada país, por conta do princípio da soberania, pode determinar sua legislação penal.

Sobre o combate à criminalidade informática a nível internacional, faz-se necessário também mencionar o *Tallinn Manual*[340], um estudo realizado sobre Direito Internacional aplicado à situações que envolvam ciberataques. O primeiro volume desse manual foi publicado no ano de 2013 e versa sobre o tema do *jus ad bellum*, normas que autorizam o uso da força entre Estados, bem como estabelecem os critérios para legitimar a ação militar. O estudo aborda convenções humanitárias e determina limites ao uso de *cyberwarfare*[341].

O segundo manual, denominado *Tallinn Manual* 2.055[342], foi publicado em 2017, e elucida o conceito de operações cibernéticas. Sydow e Magalhães[343] explicam que, enquanto o primeiro volume menciona ataques homicidas por meio de prejuízos à infraestrutura crítica de um Estado, bem como danos causados a equipamentos industriais, o segundo volume aborda situações que não se caracterizam como atos de guerra, mas que podem causar estragos a instituições públicas e privadas.

---

[338] BRASIL. **Lei nº 12.737** de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.. Brasília, DF, 30 nov. de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 13 mar. 2020.
[339] SAIN, Gustavo. *Op. cit.*, p. 23.
[340] SCHMITT, Michael N. (org.). **Manual on the International Law Applicable to Cyber Warfare**. Cambridge: Cambridge University Press, 2013.
[341] MAGALHÃES, Marcus Abreu de; SYDOW, Spencer Toth. **Cyberterrorismo: a Nova Era da Criminalidade**. Belo Horizonte: Editora D´Plácido, 2019, p. 168.
[342] SCHMITT, Michael N. (org.). **Manual 2.0 on the International Law Applicable to Cyber Operations**. Cambridge: Cambridge University Press, 2017.
[343] MAGALHÃES, Marcus Abreu de; SYDOW, Spencer Toth. *Op. cit*., p. 169.

Os referidos manuais versam sobre um assunto cada vez mais discutido no âmbito das relações internacionais: *cyberwarfare*, termo que pode traduzido para o português como "ciberguerra" ou "guerra cibernética". Trata-se de uma modalidade de conflito na qual há o uso de ferramentas disponibilizadas pelo avanço da tecnologia para atacar nações, governos e cidadãos e, de modo distinto das investidas beligerantes tradicionais, são mais sutis e difíceis de rastrear, podendo ser inseridas sigilosamente nos sistemas[344]. Como exemplos de países que constantemente estão evolvidos em conflitos caracterizados como ciberguerras, é possível mencionar os Estados Unidos e a Rússia[345].

Sobre a situação dos países que compõem o bloco do Mercosul, é preciso mencionar o Protocolo de São Luis[346], instrumento que versa sobre cooperação internacional em matéria penal. No referido protocolo há previsões sobre medidas nesse sentido, como procedimento de produção de provas, localização de pessoas e traslado de pessoas sujeitas a um processo penal. Não há, entretanto, nenhuma menção específica ao combate à delinquência informática no referido documento.

Houve um comunicado conjunto por parte dos presidentes dos Estados pertencentes do Mercosul em 2015, ressaltando a importância de encontros entre esses representantes, denominados Reuniões de Autoridades sobre Privacidade e Segurança da Informação do Mercosul[347]. Nessas reuniões há a proposição de iniciativas comuns no campo da segurança cibernética, privacidade, proteção de dados particulares e combate aos crimes informáticos. Embora esses encontros apresentem características mais técnicas do que jurídicas propriamente ditas, auxilia na elaboração de uma estratégia em comum desses países para enfrentar essa situação.

Conforme exposto, percebe-se que esse potencial que as redes informáticas apresentam por conta da imaterialidade dos dados que circulam nesse ambiente favorece a comissão de delitos

---

[344] WHAT is cyber warfare?. **IT Pro**, 16 mar. 2020. Disponível em: https://www.itpro.co.uk/security/28170/what-is-cyber-warfare. Acesso em: 14 abr. 2020.

[345] BARNES, Julian E.; SANGER, David E. Congress, Warning of Cybersecurity Vulnerabilities, Recommends Overhaul. **New York Times**, 11 mar. 2020. Disponível em: https://www.nytimes.com/2020/03/11/us/politics/congress-cyber-solarium.html. Acesso em: 22 abr. 2020.

[346] BRASIL. **Decreto nº 3.468**, de 17 maio 2000. Promulga o Protocolo de Assistência Jurídica Mútua em Assuntos Penais, assinado em San Luis, República Argentina, em 25 de junho de 1996, entre os Governos da República Federativa do Brasil, da República Argentina, da República do Paraguai e da República Oriental do Uruguai. Brasília, DF, 17 maio de 2000. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/D3468.htm. Acesso em: 22 fev. 2020.

[347] DELUCA, Santiago; DEL CARRIL, Enrique. Cooperación Internacional en Materia Penal en el Mercosur: el Cibercrimen. **Revista da Secretaria do Tribunal Permanente de Revisão**. Assunção, out. 2017, ano 5, n. 10, p. 22.

em jurisdições distintas[348]. Dessa forma, é preciso que haja uma estratégia em comum para que os Estados consigam combater essa nova forma de criminalidade, caso contrário tais atentados à integridade e segurança das informações pessoais e dos sistemas informáticos ficarão impunes. Entretanto, não se pode olvidar que cada país pode determinar sua legislação interna sobre a matéria, por conta do princípio da soberania. As iniciativas nesse sentido serão abordadas no tópico seguinte.

4.2 LEGISLAÇÃO ESTRANGEIRA

A legislação interna sobre delinquência informática de cada país depende do nível de desenvolvimento econômico e do tipo de crime cometido por meios informáticos. Conforme informações disponibilizadas por instituições policiais, atividades financeiras, como fraudes e falsificações praticados no ciberespaço[349]. Em algumas regiões do planeta, metade das atividades criminosas é relacionada ao conteúdo ilícito compartilhado, como pornografia infantil e material relativo ao terrorismo.

Os crimes relacionados à pornografia infantil são mais frequentes nos continentes americano e europeu em relação à ocorrência dessas condutas na África, na Ásia e na Oceania, o que, segundo o *United Nations Office on Drugs and Crime* (Escritório das Nações Unidas sobre Drogas e Crimes), pode estar relacionado ao foco da aplicação da lei nessas regiões do que das circunstâncias propriamente ditas[350]. Já os atos praticados no ambiente cibernético que causam danos individuais acontecem com mais regularidade na África, na América, na Ásia e na Oceania.

As perspectivas de cada Estado acerca da delinquência informática podem acarretar diversas abordagens que muitas vezes não se harmonizam umas com as outras[351]. Por exemplo, é possível que um Estado se concentre na persecução de crimes que ocorrem em seu território, sem considerar a fonte do conteúdo, ou pode optar por uma ação extraterritorial. Essas divergências existem por conta dos sistemas jurídicos adotados pelos Estados, como o *common law*, o *civil law*, a lei islâmica (*sharia*) ou um sistema misto, tal qual ocorre na China.

---

[348] ABOSO, Gustavo Eduardo. *Op. cit*., p. 45.
[349] UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Comprehensive Study on Cybercrime**, Viena, fev. 2013, p. 26. Disponível em: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. Acesso em: 22 out. 2020.
[350] *Ibidem, loc. cit.*
[351] *Ibidem*, p. 57.

Os Estados Unidos, por se tratar do país no qual "nasceu" a indústria da informática, foi um dos pioneiros na legislação voltada ao combate da delinquência no ciberespaço. No país em questão estão concentradas a maioria das empresas provedoras de serviços de Internet, tais como o Facebook, o Google, o Instagram, a Microsoft e o Twitter[352]. Dessa forma, os Estados Unidos, apesar de não ser membro da comunidade europeia, assumiu um papel fundamental na elaboração da Convenção de Budapeste[353].

A legislação estadunidense apresenta um "paralelismo normativo interessante" a respeito de algumas condutas os Estados partes desse tratado se comprometeram a considerar criminosas, conforme destaca Aboso[354]. Os Estados Unidos expressaram algumas reservas sobre o conteúdo e alcance de certos atos que configuram delitos informáticos, mais especificamente quanto à jurisdição no caso de envolvimento de cidadãos estadunidenses.

No final de 2018, os Estados Unidos realizaram uma manifestação de apoio à Convenção de Budapeste. O país e o Conselho da Europa celebraram um acordo no qual o governo estadunidense comprometeu-se a contribuir com o projeto *Cybercrime@Octopus* com a quantia de quinhentos mil dólares[355]. O projeto em questão tem como objetivo apoiar a implementação da Convenção de Budapeste em diversas partes do mundo[356].

Da mesma maneira que os Estados Unidos, o Reino Unido também ratificou a Convenção de Budapeste e implementou uma política de combate à criminalidade informática, a *National Cyber Security Strategy 2016-2021*[357]. A estratégia em questão tem como base o aperfeiçoamento dos recursos a serem utilizados nesse sentido, bem como o incentivo à cooperação internacional. Para tanto criou-se um órgão encarregado de fiscalizar os sistemas informáticos e elaborar políticas de cibersegurança, o *Information Comissioner`s Office* (Escritório do Comissário de Informação)[358].

---

[352] DUPUY, Daniela; KIEFER, Mariana. *Op. cit.*, p. 219.
[353] ABOSO, Gustavo. *Op. cit.*, p. 61.
[354] *Ibidem, loc. cit.*
[355] COUNCIL OF EUROPE. **US support to the Budapest Convention**. Estrasburgo, 25 set. 2018. Disponível em: https://www.coe.int/en/web/cybercrime/-/us-support-to-the-budapest-convention. Acesso em: 24 fev. 2020.
[356] *Idem*. **Global Project Cybercrime@Octopus**. Disponível em: https://www.coe.int/en/web/cybercrime/cybercrime-octopus. Acesso em: 24 fev. 2020.
[357] UNITED KINGDOM. **National Cyber Security Strategy 2016 to 2021**. Disponível em: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021. Acesso em: 24 fev. 2020.
[358] *Idem*. **Information Comissioner`s Office**. Disponível em: https://ico.org.uk/. Acesso em: 11 abr. 2020.

Países em desenvolvimento que vêm alcançando destaque no cenário internacional, a China e a Rússia não assinaram a Convenção de Budapeste, porém também adotaram políticas no sentido de combater a criminalidade informática. Em 1996 foi criada a Organização de Cooperação de Xangai composta pela China, Rússia, Cazaquistão, Quirguistão e Tajiquistão. Dez anos mais tarde se juntaram à referida organização a Índia e o Paquistão[359]. Essa aliança tem por finalidade garantir a segurança regional por meio do combate a movimentos extremistas, separatistas e terroristas. Durante a 22ª Sessão da Organização de Cooperação de Xangai foi realizado um acordo para combater ameaças informáticas que coloquem em risco a segurança dos países que compõem essa aliança.

No continente europeu, a Alemanha é considerada um dos países pioneiros quanto à legislação em matéria de crimes informáticos. Em 1986, foi criada a *Zweites Gesetz Bekämpfung der Wirtschaftskriminalität* [360](Lei de Combate à Criminalidade Econômica), que menciona condutas ilícitas cometidas no ambiente cibernético, como alteração de dados e sabotagem informática. O *Strafgesetzbuch*[361] (Código Penal Alemão) possui normas que versam sobre crimes informáticos, como a espionagem e as condutas contempladas na referida lei. A Polícia Federal da Alemanha elabora, desde o ano de 2010, relatórios anuais sobre a ocorrência de crimes informáticos no país[362].

Outro país que possui previsão legislativa sobre crimes informáticos desde a década de 1980 é a França, que, com a Lei nº 88-19[363], de 1988, tipificou as seguintes condutas: acesso fraudulento a um sistema informático; sabotagem informática; destruição de dados; falsificação de documentos informatizados. Mais recentemente, a Lei nº 2004-575[364], que trata do comércio eletrônico na França, abordou situações que configuram fraudes informáticas. Em 2009 foi criada a Lei nº 2009-669 ou *Loi Haute Autorité pour la Diffusion*

[359] ABOSO, Gustavo. *Op. cit.*, p. 64-65.
[360] ALEMANHA. **Zweites Gesetz Bekämpfung der Wirtschaftskriminalität**, 23 maio 1986. Disponível em: https://www.bgbl.de/xaver/bgbl/text.xav?SID=&tf=xaver.component.Text_0&tocf=&qmf=&hlf=xaver.component.Hitlist_0&bk=bgbl&start=%2F%2F*%5B%40node_id%3D%27379873%27%5D&skin=pdf&tlevel=-2&nohist=1. Acesso em: 24 fev. 2020.
[361] *Idem*. **Strafgesetzbuch**, 15 maio 1871. Disponível em: https://www.gesetze-im-internet.de/stgb/. Acesso em: 24 fev. 2020.
[362] *Idem*. **Bundeslagebilder Cybercrime**. Disponível em: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html. Acesso em 24 fev. 2020.
[363] FRANÇA. **Loi n° 88-19** du 5 janvier 1988 relative à la fraude informatique. Disponível em: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000875419&categorieLien=id. Acesso em: 25 fev. 2020.
[364] *Idem*. **Loi n° 2004-575** du 21 juin 2004 pour la confiance dans l'économie numérique. Disponível em: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164. Acesso em: 24 fev. 2020.

des Œuvres et la Protection des droits sur Internet, mais conhecida pela sigla HADOPI (Alta Autoridade da Difusão de Obras e da Proteção dos Direitos na Internet)[365], para assegurar o cumprimento dos direitos autorais no âmbito da Internet.

Na Itália, a legislação com o intuito de combater a delinquência informática surgiu no início da década de 1990, com o Decreto-lei nº 518[366], de 29 de dezembro de 1992, e a Lei nº 547[367], de 23 de dezembro de 1993. Essas leis ampliaram a redação de tipos penais já previstos para abarcar crimes informáticos impróprios e criminalizou condutas como ataques cibernéticos e fraudes informáticas. O tipo penal denominado "invasão de domicílio", previsto no art. 615 do Código Penal Italiano[368], foi ampliado no ano de 2008 para contemplar a conduta de "invasão de IP", que consiste em uma ação com o intuito de causar prejuízos ao sistema informático alheio.

Sobre a região ibérica da Europa, é possível mencionar que, em Portugal, existe a Lei nº 109, de agosto de 1991[369], tipificando certas condutas cometidas no ambiente cibernético, como o acesso indevido a sistemas informáticos, dano informático e reproduções indevidas de programas de computador. Há um caso de bastante repercussão atualmente em Portugal que envolve a acusação de um hacker denominado Rui Pinto[370]. Ele conseguiu obter acesso a dispositivos informáticos de jogadores de futebol e empresários, divulgando mensagens e documentos com informações sobre fraudes cometidas no meio esportivo. O hacker está preso desde março de 2019 por conta de crimes como violação de correspondência, sabotagem informática e tentativa de extorsão.

Já na Espanha, o Código Penal de 1995[371] sofreu alterações para contemplar condutas que são consideradas crimes informáticos para esse país, tais como alteração e acesso indevidos de

---

[365] *Idem*. **Loi nº 2009-669** du 12 juin 2009, Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet. Disponível em: https://www.hadopi.fr/en. Acesso em: 24 fev. 2020.

[366] ITÁLIA. **Decreto Legislativo 29 dicembre 1992, n. 518**. Disponível em: https://www.gazzettaufficiale.it/eli/id/1992/12/31/092G0565/sg. Acesso em: 24 fev. 2020.

[367] *Idem*. **Legge 23 dicembre 1993 n. 547**. Disponível em: https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=1993-12-30&atto.codiceRedazionale=093G0633&elenco30giorni=false. Acesso em: 24 fev. 2020.

[368] *Idem*. **Código Penal – Decreto 19 ottobre 1930, n. 1398**. Roma, 19 outubro de 1930. Disponível em: https://www.altalex.com/documents/codici-altalex/2014/10/30/codice-penale. Acesso em: 24 fev. 2020.

[369] PORTUGAL. **Lei n.º 109/91.** Lei da criminalidade informática. Disponível em: https://dre.pt/pesquisa/-/search/674438/details/maximized. Acesso em: 24 fev. 2020.

[370] CASTRO, Luiz Felipe. O Snowden da Bola: Quem é o hacker português por trás do Football Leaks, o vazamento de milhões de documentos sigilosos que revelou negociatas e falcatruas dentro e fora dos gramados. **Veja**, ed. 2675, 26 fev. 2020, ano 53, n. 9, p. 78-79.

[371] ESPANHA. **Ley Orgánica 10/1995**, de 23 de noviembre de 1995, del Código Penal. Disponível em: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444. Acesso em 24 fev. 2020.

dados e fraude informática. De la Fuente[372] explica que tais modificações foram fundamentais para adaptar uma legislação defasada ao desenvolvimento tecnológico e às formas de cometimento de crimes proporcionadas pelo mesmo. A vulnerabilidade dos usuários de dispositivos informáticos, principalmente os menores de idade, para a autora, se deve à sua utilização massiva e ausência de uma política efetiva de prevenção dos riscos no ambiente informático.

O primeiro país da América do Sul a atualizar sua legislação para tratar dos delitos informáticos foi o Chile[373]. A Lei 19.223[374], de 7 de junho de 1993, também chamada de Lei Própria de Crimes Informáticos tipifica atos como inutilização de sistemas de processamento de dados e acesso indevido de informações confidenciais.

A Argentina, por sua vez, manifestou-se contra a criminalidade informática com o advento da Lei nº 26.388/2008[375], instrumento responsável por alterar o Código Penal[376], que incorporou algumas condutas delitivas praticadas por meios informáticos, tais como o acesso indevido a sistemas informáticos e danos informáticos. Além dessa lei, em 2013 a Lei nº 26.904[377] introduziu o crime de *grooming* e, em 2018, a Lei 27.436[378] modificou o art.128 do Código Penal.

A Subsecretaria de Justiça e Política Criminal, órgão vinculado ao Ministério de Justiça e Direitos Humanos da Argentina criou em 2016 o Programa Nacional Contra a Criminalidade Informática (PNCCI)[379]. A finalidade desse programa é fomentar políticas que melhorem as

---

[372] FUENTE, Elvira Tejada de la. Novedades en la Tipificación de Determinados Delitos Vinculados a la Criminalidad Informática en el Código Penal Español; Evolución Legislativa y Adaptación a la Normativa Internacional. In: DUPUY, Daniela (Direção); KIEFER, Mariana (Coordenação). **Cibercrimen: Aspectos de Derecho penal y procesal penal. Cooperación Internacional. Recolección de evidencia digital. Responsabilidad de los provedores de servicios de Internet**. Buenos Aires: Editorial B de F, 2019, p. 37.

[373] JESUS, Damásio de.; MILAGRE, José Antonio. *Op. cit*., p. 68.

[374] CHILE. **Ley 19.223** de 7 de junio de 1993. Disponível em: https://www.leychile.cl/Navegar?idNorma=30590. Acesso em: 26 fev. 2020.

[375] ARGENTINA. **Ley 26.388,** de junio 24 de 2008. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm. Acesso em: 26 fev. 2020.

[376] *Idem*. **Código Penal de la Nación Argentina**. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm. Acesso em: 26 fev. 2020.

[377] *Idem*. **Ley 26.904**, 04 de diciembre 2013. Disponivel em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/220000-224999/223586/norma.htm. Acesso em: 26 fev. 2020.

[378] *Idem*. **Ley 27.436**, 21 de marzo de 2018. Disponível em: https://www.argentina.gob.ar/normativa/nacional/ley-27436-309201. Acesso em: 26 fev. 2020.

[379] *Idem*. **Resolución Ministerial 69/16 - Creación del Programa Nacional Contra la Criminalidad Informática en la órbita del Ministerio de Justicia**, 11 de marzo de 2016. Disponível em: http://www.saij.gob.ar/creacion-programa-nacional-contra-criminalidad-informatica-orbita-ministerio-justicia-

respostas do sistema penal do país frente à criminalidade informática. Dentre as medidas adotadas pelo PNCCI estão o incentivo à cooperação internacional para esse objetivo e capacitar os operadores do sistema penal frente aos desafios suscitados pelos crimes informáticos.

O Código Penal peruano[380] é recente, promulgado em abril de 1991, e já apresentava a necessidade de tratar dos delitos praticados no ciberespaço tendo tipificado a conduta de "furto informático", sendo uma modalidade de furto agravado. Contudo, por conta de uma demanda social em relação ao uso indevido da informática, o Congresso Nacional do Peru percebeu a necessidade de criar novos crimes e aumentaram a pena de outros cometidos por meios informáticos. A Lei 27.309 de julho de 2000[381] estabeleceu novos tipos penais, como a destruição de base de dados e a alteração de sistemas informáticos.

4.3 LEGISLAÇÃO BRASILEIRA

Conforme mencionado anteriormente, o Brasil não aderiu à Convenção de Budapeste até o presente momento, o que não significa que se omitiu em relação ao combate à criminalidade informática. Em 2018, membros do Ministério Público Federal (MPF) participaram da Conferência Internacional sobre Cooperação Judiciária em Cibercrime e Evidência Eletrônica, realizada na cidade de Haia, na Holanda, um evento que reuniu representantes de sessenta e seis países[382].

De acordo com informações disponibilizadas no site do MPF, a ratificação do referido tratado seria um passo relevante na investigação de crimes cometidos por meio de plataformas digitais, como aplicativos de mensagens instantâneas[383]. Esse avanço seria relevante para

---

nv14027-2016-03-11/123456789-0abc-720-41ti-lpssedadevon. Acesso em: 26 fev. 2020.

[380] PERU. **Código Penal Peruano**. Disponível em: http://spij.minjus.gob.pe/content/publicaciones_oficiales/img/CODIGOPENAL.pdf. Acesso em 26 fev. 2020.

[381] *Idem*. **Ley n° 27.309** de 17 de julio de 2000. Modifícase el Título V del Libro Segundo del Código Penal, promulgado por Decreto Legislativo Nº 635**.** Disponível em: https://www.gob.pe/institucion/pcm/normas-legales/292284-27309. Acesso em: 26 fev. 2020.

[382] BRASIL. Em conferência internacional, MPF defende cooperação como forma de combater o cibercrime. Ministério Público Federal. **Ministério Público Federal**, 14 mar. 2018. Disponível em: http://www.mpf.mp.br/pgr/noticias-pgr/em-conferencia-internacional-mpf-defende-cooperacao-como-forma-de-combater-o-cibercrime. Acesso em: 13 mar. 2020.

[383] *Ibidem, loc. cit.* Disponível em: http://www.mpf.mp.br/pgr/noticias-pgr/em-conferencia-internacional-mpf-defende-cooperacao-como-forma-de-combater-o-cibercrime. Acesso em: 13 mar. 2020.

solucionar, por exemplo, as situações de conflito entre a justiça e o Facebook, mencionadas anteriormente[384].

O MPF tem empregado esforços no sentido de incluir o Brasil na Convenção de Budapeste desde o ano de 2004, expedindo orientações e elaborando acordos tanto no âmbito nacional quanto no internacional[385]. Espera-se que a adesão do país à Convenção aconteça em breve, sendo um fator favorável a intensificação das negociações após o estabelecimento da parceria entre a Secretaria de Cooperação Internacional (SCI) e o Grupo de Apoio sobre Criminalidade Cibernética da Câmara Criminal do MPF (GACC/2CCR), que passaram a se articular conjuntamente em busca da adesão.

É preciso ressaltar que, até o ano de 2012, não havia legislação específica no Brasil para tratar de crimes informáticos. O Direito Penal, malgrado seja considerado a *ultima ratio* para resolução de conflitos, em território brasileiro foi a medida adotada inicialmente para lidar com a questão da delinquência informática. Inclusive, essa providência foi adotada de maneira bastante célere por conta de uma situação que envolveu uma atriz famosa.

Em maio de 2012, fotos da atriz Carolina Dieckmann nua começaram a circular na Internet[386]. Pouco tempo depois, Dieckmann se manifestou, por meio de seu advogado, declarando que havia sido alvo de chantagem por cerca de um mês antes das fotos serem disponibilizadas na rede[387]. O hacker que havia invadido o computador da atriz exigiu a quantia de dez mil reais para não divulgar as fotos.

Anteriormente, uma situação similar havia acontecido com outra atriz. A estadunidense Scarlet Johanson teve imagens suas divulgadas na Internet nas quais ela estava despida em 2011[388]. Tratavam-se de fotos tiradas por ela mesma, com seu celular, em frente a um espelho em sua casa. O hacker responsável pela disponibilização das imagens foi identificado, tendo

---

[384] WHATSAPP bloqueado: Relembre todos os casos de suspensão do app. *Op. cit*. Acesso em: 13 mar. 2020.
[385] BRASIL. Conselho da Europa convida o Brasil para compor a Convenção de Budapeste sobre o Cibercrime. **Ministério Público Federal**, 13 dez. 2019. Disponível em: http://www.mpf.mp.br/pgr/noticias-pgr/conselho-da-europa-convida-o-brasil-para-compor-a-convencao-de-budapeste-sobre-o-cibercrime. Acesso em: 13 mar. 2020.
[386] DIECKMANN é assunto mais falado do Twitter após vazamento de fotos. **G1**, 04 maio 2012. Disponível em: http://g1.globo.com/tecnologia/noticia/2012/05/dieckman-e-assunto-mais-falado-do-twitter-apos-vazamento-de-fotos.html. Acesso em: 01 mar. 2020.
[387] MENDES, Priscilla. Dieckmann foi chantageada em R$ 10 mil por fotos, diz advogado. **G1**, 05 maio 2012. Disponível em: http://g1.globo.com/tecnologia/noticia/2012/05/dieckmann-foi-chantageada-em-r10-mil-devido-fotos-diz-advogado.html. Acesso em: 01 mar. 2020.
[388] DIECKMANN é assunto mais falado do Twitter após vazamento de fotos. *Op. cit*. . Disponível em: http://g1.globo.com/tecnologia/noticia/2012/05/dieckman-e-assunto-mais-falado-do-twitter-apos-vazamento-de-fotos.html. Acesso em: 01 mar. 2020.

sido condenado a dez anos de prisão, além de pagamento de indenização, por ter feito o mesmo com imagens de outras celebridades, como a cantora Christina Aguilera e a atriz Mila Kunis[389]. O autor dos crimes obtinha acesso a tais imagens invadindo as contas de e-mail das vítimas e foi considerado culpado de nove acusações criminais, incluindo roubo de identidade, escutas telefônicas, acesso não autorizado e danos a um computador protegido, condutas tipificadas na legislação estadunidense.

Carolina Dieckmann, apesar de ter sido chantageada pelos hackers que divulgaram suas fotos íntimas, decidiu não agir em conformidade com as demandas dos criminosos e denunciou o caso à polícia[390]. Ela passou sete horas em uma delegacia onde relatou que desconfiava que as fotos publicadas no Brasil e em dois sites estrangeiros haviam sido obtidas no período em que o computador foi enviado para manutenção. O advogado da atriz notificou o Google para proibir a busca das imagens no provedor de pesquisa. Ademais, os sites de pornografia situados em Londres e nos Estados Unidos que divulgaram as fotos de Dieckmann também foram identificados.

Essas situações mencionadas anteriormente só corroboram a declaração concedida pelo criador do sistema *World Wide Web*, Timothy Beners-Lee, na qual ele comentou que considera a Internet um local de abusos generalizados contra mulheres[391]. Além de possuírem menos chances de acessar a Internet em países pouco desenvolvidos, mulheres são mais propensas a sofrer ataques nesse ambiente, caracterizando mais um espaço onde ocorre a violência de gênero.

Conforme as investigações sobre a situação envolvendo Dieckmann foram avançando, a polícia do Rio de Janeiro chegou a uma cidade no interior de São Paulo chamada Macatuba[392]. Os policiais da Delegacia de Repressão Contra Crimes de Internet, munidos de um mandado de busca e apreensão, encontraram um dos autores da estratégia de invasão informática e extorsão contra Carolina Dieckmann em um quarto com diversas imagens de

[389] HACKER que roubou fotos de Scarlett Johansson pega 10 anos de prisão. **G1**, 17 dez. 2012. Disponível em http://g1.globo.com/tecnologia/noticia/2012/12/hacker-que-roubou-fotos-de-scarlet-johansson-pega-10-anos-de-prisao.html. Acesso em: 01 mar. 2020.

[390] POLÍCIA ouve empresa de informática sobre fotos de Carolina Dieckmann. **G1**, 07 maio 2012. Disponível em: http://g1.globo.com/rio-de-janeiro/noticia/2012/05/policia-ouve-empresa-de-informatica-sobre-fotos-de-carolina-dieckmann.html. Acesso em: 01 mar. 2020.

[391] INTERNET alimenta abusos contra mulheres, alerta seu inventor. **Istoé**, 12 mar. 2020. Disponível em: https://istoe.com.br/internet-alimenta-abusos-contra-mulheres-alerta-seu-inventor/. Acesso em: 12 mar. 2020.

[392] HACKERS que roubaram fotos de Carolina Dieckmann são presos. **Techmundo**, 14 maio 2012. Disponível em: https://www.tecmundo.com.br/ataque-hacker/23514-*hackers*-que-roubaram-fotos-de-carolina-dieckmann-sao-presos.htm. Acesso em: 01 mar. 2020.

pessoas famosas. O rapaz havia acabado de formatar uma das máquinas que continham as fotos da atriz.

Foi esclarecido que o acesso às imagens não ocorreu quando o computador de Dieckmann foi levado para manutenção, havendo, na verdade, uma fraude cometida por meios informáticos[393]. A atriz recebeu um spam, uma mensagem não solicitada, e acessou-o, possibilitando assim que um *malware* fosse instalado em seu computador. Por meio desse programa malicioso, os hackers conseguiram invadir o dispositivo e ter acesso às fotos íntimas. Cinco pessoas estavam envolvidas nas práticas delituosas e foram indiciadas por crimes de difamação, furto e extorsão.

Muito provavelmente, devido ao fato de que a situação em que houve o acesso não autorizado a um dispositivo informático e a divulgação de imagens íntimas de uma pessoa famosa, o Poder Público tomou providências de forma bastante rápida, o que talvez não acontecesse se a vítima não fosse uma celebridade. No final do ano 2012, meses após a divulgação das fotos e da investigação dos crimes, a então Presidente da República sancionou duas leis relacionadas a crimes informáticos.

Antes da Lei nº 12.737/2012[394], que ficou conhecida como Lei Carolina Dieckmann, por conta da repercussão da situação vivida pela atriz, a conduta de invasão informática não era considerada um crime. Dessa forma, os autores das condutas delituosas cuja vítima foi a referida atriz não foram punidos por essa prática. A lei modificou o art. 154, que tratava somente de violação de sigilo profissional, acrescentando o art. 154-A. O mencionado artigo descreve o seguinte crime: invasão de dispositivo informático alheio, conectado ou não à rede de computadores, por meio de violação indevida de mecanismo de segurança e para obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. Ao autor dessa conduta é atribuída pena de detenção de três meses a um ano e multa.

Caso essa ação delituosa tenha como consequência prejuízo econômico para a vítima, se for praticada contra autoridade ou se uma comunicação particular, que contenha informações

[393] *Idem*. Disponível em: https://www.tecmundo.com.br/ataque-hacker/23514-*hackers*-que-roubaram-fotos-de-carolina-dieckmann-sao-presos.htm. Acesso em: 01 mar. 2020.
[394] BRASIL. **Lei nº 12.737** de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.. Brasília, DF, 30 nov. de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 13 mar. 2020.

sigilosas comerciais ou industriais cabe a punição não só para o autor da conduta como também para o indivíduo que produz ou distribui ferramentas utilizadas nesse sentido.

Além da Lei Carolina Dieckmann, no Brasil há a Lei nº 12.735/2012[395], que também versa sobre crimes informáticos. A legislação ficou conhecida como Lei Azeredo, por ter sido proposta pelo ex-senador Eduardo Azeredo. Após sofrer algumas modificações, pois o projeto de lei visava a criminalização de diversas condutas, mas essas partes foram vetadas, a Lei Azeredo estabeleceu que os órgãos da polícia judiciária devem estruturar setores e equipes para atuarem especificamente na repressão à criminalidade no ambiente cibernético.

Ressalte-se que, embora a Lei nº 12.735/2012 já tenha sido sancionada há alguns anos, ainda há poucas repartições públicas, como delegacias, por exemplo, especializadas no combate aos delitos informáticos. É necessário que o Estado realize mais investimentos nesse sentido, pois a criminalidade no âmbito cibernético só faz aumentar e a população brasileira não está suficientemente amparada. As pessoas ainda não se sentem seguras para denunciar crimes informáticos como acontece com crimes "comuns".

A ausência de comunicação dessa criminalidade às autoridades competentes deve-se a três motivos principais, segundo leciona Sydow[396]. O primeiro deles é que pessoa lesada por um delito informático se sente incompetente por não ter conhecimento o suficiente sobre informática, de modo que a vítima se sente constrangida para denunciar esses crimes. Já a segunda razão está relacionada somente às pessoas jurídicas, como instituições bancárias e lojas, que ficam apreensivas ao comunicar a ocorrência de crimes informáticos e, com isso, sofrer danos reputacionais, pois o público pode não ter mais confiança na organização. Por fim, o terceiro motivo é a descrença no Poder Público para punir os autores de delitos informáticos, bem como a reparação à pessoa lesada, que raramente consegue obter alguma reparação.

Faz-se necessário ressaltar o trabalho de outros agentes sociais para diminuir a criminalidade informática. A *SaferNet Brasil*, associação civil de direito privado, sem fins lucrativos ou

[395] BRASIL. **Lei nº 12.735** de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Brasília, DF, 30 nov. de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm. Acesso em: 13 mar. 2020.
[396] SYDOW, Spencer. *Op. cit*., p. 60.

econômicos e sem vinculação político partidária, religiosa ou racial atua para promover e salvaguardar os Direitos Humanos na Internet no Brasil desde a sua fundação em 2005[397].

A associação possui um projeto em parceria com o MPF denominado Central Nacional de Denúncias de Crimes Cibernéticos. De acordo com dados contidos no site da Safernet, em 14 anos a associação recebeu e processou 4.134.808 denúncias anônimas, envolvendo 790.390 páginas (URLs) distintas escritas em 9 idiomas e hospedadas em 73.000 domínios diferentes, atribuídos para 104 países em 6 continentes[398]. Em 2017, foram recebidas 63.698 denúncias de crimes realizadas por usuários anônimos. No ano seguinte, o número de denúncias aumentou para 133.732. Os três crimes mais denunciados em 2018 foram: pornografia infantil (60.002 denúncias); conteúdos de apologia e incitação à violência e crimes contra a vida (27.716 denúncias); violência contra mulheres ou misoginia (16.717 denúncias) [399].

Em uma matéria veiculada pelo jornal Estado de Minas Gerais em 2019, consta que, de acordo com dados coletados pela *SaferNet Brasil* e pelo MPF em 2018, uma média de 366 crimes informáticos são registrados diariamente[400]. Há dezesseis delegacias especializadas em delitos cometidos por meios informáticos no Brasil nos seguintes estados: Bahia, Espírito Santo, Maranhão, Mato Grosso, Minas Gerais, Pará, Paraná, Pernambuco, Piauí, Rio Grande do Sul, São Paulo, Sergipe, Rio de Janeiro, Tocantins e Distrito Federal. Apenas o estado de São Paulo possui duas delegacias, uma que atende somente demandas relacionadas a crimes informáticos e outra especializada em crimes contra a dignidade sexual de vulneráveis, mas que se ocupa de delitos informáticos praticados no referido contexto[401]. Trata-se ainda de um número pequeno de delegacias para a quantidade de crimes informáticos que ocorrem no país.

A ANATEL informa que tais delegacias atuam em conjunto com delegacias da polícia civil e, caso não exista uma delegacia especializada na cidade onde a vítima se encontra, o órgão

---

[397] INSTITUCIONAL. **SaferNet Brasil**. Disponível em: https://new.safernet.org.br/content/institucional. Acesso em: 13 mar. 2020.

[398] DATASAFER. 30.389 atendimentos e 4.134.808 denúncias. **SaferNet**. Disponível em: https://indicadores.safernet.org.br/indicadores.html. Acesso em: 18 maio 2020.

[399] DENÚNCIAS de crimes online contra mulheres sobem 1600% no Brasil em 2018. **Revista Painel Político**, 07 de fevereiro de 2019. Disponível em: https://revista.painelpolitico.com/denuncias-de-crimes-online-contra-mulheres-sobem-1600-no-brasil-em-2018/. Acesso em: 13 mar. 2020.

[400] CRIMES cibernéticos disparam e expõem fragilidade tecnológica no Brasil. **Estado de Minas**, Belo Horizonte, 04 ago. 2019. Disponível em: https://www.em.com.br/app/noticia/politica/2019/08/04/interna_politica,1074689/crimes-ciberneticos-disparam-expoem-fragilidade-tecnologica-no-brasil.shtml. Acesso em: 13 abr. 2020.

[401] DELEGACIAS Cibercrimes. **SaferNet**. Disponível em: https://new.safernet.org.br/content/delegacias-cibercrimes. Acesso em: 13 abr. 2020.

orienta a procurar a delegacia mais próxima[402]. De acordo com um relatório elaborado pela empresa *PSafe*, especializada em serviços de segurança no ambiente cibernético, referente ao segundo trimestre de 2018, a região sudeste foi a que detectou o maior número de links maliciosos por habitante[403].

Mesmo com um número reduzido de delegacias especializadas, as pessoas têm buscado esses órgãos cada vez mais para realizar denúncias, tendo o número de ocorrências registradas aumentado 110% de 2017 para 2018 segundo dados levantados pela SaferNet e pelo MPF[404]. Na delegacia especializada em crimes informáticos situada no estado de Goiás, por exemplo, foi registrado um aumento da quantidade de ocorrências registradas de 2017 para 2018: 1,4 para 3,3 ocorrências por mês. Os crimes mais frequentes são calúnia, difamação, injúria, pornografia infantil e estelionatos, a maior parte das ocorrências concentrada em Goiânia[405].

Mais recentemente, no ano de 2019, foi aberta pela Polícia Federal uma investigação batizada de Operação *Spoofing* devido à técnica utilizada pelos hackers para acessar o celular das autoridades envolvidas na Operação Lava Jato[406]. A Polícia Federal chegou a alguns suspeitos por elaborar uma estratégia para invadir as contas do aplicativo de troca de mensagens Telegram das pessoas retromencionadas[407]. Ocorre que o método utilizado não violou um mecanismo de segurança do dispositivo, tendo apenas tirado proveito de uma falha no sistema de proteção do aplicativo, mas a questão sobre o método utilizado para acessar o aparelho será explanada mais à frente.

A troca de mensagens entre Moro e outras autoridades foi publicada no site *The Intercept*, fundado pelo jornalista Glenn Greenwald, que já havia divulgado documentos confirmando que o governo dos Estados Unidos monitorava conversas sigilosas de milhares de políticos,

---

[402] CRIMES cibernéticos: descubra como você pode se proteger de ataques na internet. **Agência Nacional de Telecomunicações**, 27 ago. 2019. Disponível em . Acesso em: 13 abr. 2020.

[403] RELATÓRIO da Segurança Digital – segundo semestre de 2018. **PSafe**. Disponível em https://www.psafe.com/dfndr-lab/wp-content/uploads/2018/08/Relat%C3%B3rio-da-Seguran%C3%A7a-Digital-no-Brasil-2-trimestre-2018.pdf. Acesso em: 13 abr. 2020.

[404] FERNANDES. Augusto. Crimes virtuais e ataques cibernéticos mais do que dobram em um ano. **Correio Braziliense**, 04 ago. 2019. Disponível em: https://www.correiobraziliense.com.br/app/noticia/politica/2019/08/04/interna_politica,775357/crimes-virtuais-e-ataques-ciberneticos-mais-do-que-dobram-em-um-ano.shtml. Acesso em: 13 abr. 2020.

[405] OLIVEIRA, Rafael. Cinco tipos de crimes digitais devem dominar a internet brasileira em 2019. **Jornal Opção**, 29 de setembro de 2019. Disponível em: https://www.jornalopcao.com.br/reportagens/cinco-tipos-de-crimes-digitais-devem-dominar-a-internet-brasileira-em-2019-212858/. Acesso em: 13 de abril de 2020. https://www.anatel.gov.br/consumidor/noticias/698-crimes-ciberneticos-saiba-como-se-proteger

[407] PRAZERES, Leandro. PF indicia seis *hackers* por invasão de celulares que atingiu Sergio Moro. **O Globo**, Brasília, 19 dez. 2019. Disponível em: https://oglobo.globo.com/brasil/pf-indicia-seis-*hackers*-por-invasao-de-celulares-que-atingiu-sergio-moro-24147902. Acesso em: 01 mar. 2020.

funcionários públicos de alto escalão e empresários de todo o mundo[408]. Ao ser questionado sobre a procedência das mensagens expostas no *The Intercept*, o jornalista disse que teve contato com a fonte apenas virtualmente e que desconhecia a identidade do hacker[409]. Greenwald foi denunciado na Operação *Spoofing*, pois, segundo investigadores, tinha conhecimento que a atividade criminosa não havia cessado[410].

Trata-se de um caso de hacktivismo, termo que vem da fusão dos termos "hacker" e "ativismo", uma maneira de se insurgir contra governos e empresas por meio de ataques informáticos com o intuito de causar impacto[411]. Contudo, antes de ser uma situação de hacktivismo, é uma violação à intimidade dessas pessoas que tiveram os smartphones invadidos. Afinal, os celulares poderiam ser utilizados para outros fins que não fossem somente profissionais. A questão do direito à intimidade será abordada na seção seguinte.

5 A PROTEÇÃO DE MATERIAL DE CUNHO ÍNTIMO E SEUS ASPECTOS PENAIS

O avanço da tecnologia informática apresentou como uma de suas consequências novas noções acerca dos âmbitos público e privado. A exposição das pessoas vem aumentando, bem como a troca de informações se torna cada vez mais intensa, devido à popularização de dispositivos com acesso à Internet. Os indivíduos permitem que aspectos de suas vidas privadas sejam conhecidos por mais pessoas, que não necessariamente fazem parte de seus círculos sociais, o que leva a crer que a ideia de intimidade está sendo modificada para se adaptar à época atual.

Contudo, é preciso lembrar que o legislador caminha em um ritmo mais devagar do que o compasso das mudanças acarretadas pela evolução tecnológica. Trata-se de uma atividade ininterrupta, conforme destaca Paulo José da Costa Júnior[412], que compara a tarefa do

---

[408] SCHMITT, Paula. Vaza Jato, Glenn Greenwald e uma coincidência intrigante – parte 3. **Poder 360**, 20 fev. 2020. Disponível em: https://www.poder360.com.br/opiniao/midia/vaza-jato-glenn-greenwald-e-uma-coincidencia-intrigante-parte-3-por-paula-schmitt/. Acesso em: 01 mar. 2020.

[409] MOLICA, Fernando; RESENDE, Leandro. Glenn Greenwald revela diálogo com fonte de mensagens vazadas. **Veja**, 26 jul. 2019. Disponível em: https://veja.abril.com.br/politica/glenn-greenwald-revela-dialogo-com-fonte-de-mensagens-vazadas/. Acesso em: 01 mar. 2020.

[410] CAMAROTTO, Murillo; MARTINS, Luísa; PERON, Isadora. Glenn Greenwald é denunciado junto com *hackers* na Operação Spoofing. **Valor**. Brasília, 21 jan. 2020. Disponível em: https://valor.globo.com/politica/noticia/2020/01/21/glenn-greenwald-e-denunciado-junto-com-*hackers*-na-operacao-spoofing.ghtml. Acesso em: 01 mar. 2020.

[411] PROTESTOS na Internet: Conheça 7 casos recentes de ativismo hacker. **Canaltech**, 21 set. 2017. Disponível em: https://canaltech.com.br/internet/protestos-na-internet-conheca-7-casos-recentes-de-ativismo-hacker-100796/. Acesso em: 01 mar. 2020.

[412] COSTA JÚNIOR, Paulo José da. **O Direito de Estar Só: A tutela Penal do direito à intimidade**, 3a ed. São Paulo: Siciliano Jurídico, 2004, p. 13.

legislador ao mito grego de Sísifo, mortal condenado pelos deuses a empurrar uma pedra que, ao chegar no topo da montanha, sempre voltava a cair. Assim, tanto o legislador quanto o jurista devem estar sempre em busca da atualização para prestar um melhor serviço à sociedade.

Mesmo considerando que há um aumento desproporcional realizado por alguns cientistas sobre o futuro da sociedade, Rodríguez[413] concorda que a capacidade de transmissão de dados e a facilidade de comunicação exigem uma resposta por parte do Direito. Essas novas formas de relações interpessoais que acarretam novos riscos para a intimidade, segundo já previsto na teoria de Beck[414], resultam em uma maior preocupação no sentido de proteger esse bem jurídico.

Há muito algumas instituições, como o Estado e as organizações empresariais estão cientes de que possuir informação acarreta mais poder sobre a sociedade em geral[415]. O conhecimento sobre as preferências e necessidades do público permite manobras no mercado e, durante situações de conflito armado, significam uma vantagem sobre a parte adversária. Entretanto, os dispositivos informáticos atuais, devido a um grau mais elevado se sofisticação, oferecem a possibilidade de conhecer as atividades cotidianas de uma pessoa sem a necessidade de fiscalizá-la o tempo todo.

É possível dividir a concepção da intimidade em duas vertentes, sendo uma a sua expressão interior e outra relativa à exterioridade[416]. Enquanto a intimidade exterior seria o ensimesmamento no âmbito da coletividade, a interior consiste na sensação experimentada pelo indivíduo quando não está acompanhado de outras pessoas, o que não significa solidão, mas um sentimento mais próximo da noção de "solitude". Essa palavra designa a situação na qual a pessoa se isola de forma proposital para refletir, sem que isso acarrete um sentimento negativo[417].

Talvez esse estado de natureza psíquica da solitude seja o mais difícil de alcançar ultimamente, porque o comportamento social da atualidade exige que as pessoas passem cada

[413] RODRÍGUEZ, Víctor Gabriel. **Tutela Penal da Intimidade: perspectivas da atuação penal na sociedade da informação**. São Paulo: Atlas, 2008, p. 1.
[414] BECK, Ulrich. *Op. cit.*, p. 14.
[415] RODRÍGUEZ, Víctor Gabriel. *Op. cit.*, p. 2.
[416] COSTA JÚNIOR, Paulo José da. *Op. cit.*, p. 14.
[417] SOLITUDE. In: **Dicionário Online de Português**. Disponível em: https://www.dicio.com.br/solitude/. Acesso em: 04 mar. 2020.

vez mais tempos conectadas. Para encontrar um equilíbrio saudável, especialistas sugerem que se faça uma "desintoxicação digital", expressão que, inclusive, está prevista no dicionário de Oxford desde 2013[418]. O procedimento consiste em passar ao menos três dias sem ter acesso ao "mundo tecnológico" e assim curar o "vício"[419].

A explicação do conceito de intimidade depende da comparação a noções parecidas, tais como confidencialidade, segredo e privacidade, segundo elucida Rodríguez[420]. Malgrado essas expressões sejam utilizadas como sinônimos de "intimidade", não há consenso sobre o assunto, de forma que é possível atribuir uma dimensão jurídica a cada um desses termos.

A intimidade não se relaciona diretamente à noção de confidencialidade, uma vez que salvaguardar a intimidade não significa possuir um conhecimento restrito sobre a vida de alguém[421]. A primeira trata-se de uma maneira de expressar a liberdade, enquanto a segunda constitui uma forma ou instrumento de proteção. Em suma: o segredo é intrínseco à noção de intimidade, ainda que possa servir como meio para que ela seja exercida.

Faz-se relevante também realizar a distinção entre as noções de intimidade e vida privada. A própria Constituição Federal[422] brasileira menciona esses conceitos no inciso X do seu art. 5º, de acordo com o qual são invioláveis "a intimidade, a vida privada, a honra e a imagem das pessoas". Considerando o princípio basilar da hermenêutica *verba cum effectu sunt accipienda* (a lei não contém palavras inúteis), é preciso atentar para a diferença entre esses termos.

A distinção entre direito à intimidade e direito à proteção vida privada é realizada, com base na doutrina italiana, na obra de Paulo José da Costa Júnior[423]. A tutela da vida privada consiste no direito a evitar que outras pessoas venham a ter conhecimento das particularidades da vida alheia. Dessa forma, o indivíduo goza do direito de obstar que outros intervenham na esfera particular de sua existência. O direito à intimidade sucederia, assim, o direito à

---

[418] DIGITAL DETOX. In: **Lexico**, Oxford. Disponível em: https://www.lexico.com/definition/digital_detox. Acesso em: 04 mar. 2020.

[419] QUANTO tempo você precisa ficar longe do celular e das redes para uma 'desintoxicação digital' efetiva?. **BBC**, 27 mar. 2017. Disponível em: https://www.bbc.com/portuguese/internacional-39402166. Acesso em: 04 mar. 2020.

[420] RODRÍGUEZ, Víctor Gabriel. *Op. cit.*, p. 2.

[421] *Ibidem*, p. 27.

[422] BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 04 mar. 2020.

[423] RODRÍGUEZ, Víctor Gabriel. *Op. cit.*, p. 30.

proteção da vida privada, pois consistira no impedimento da divulgação de notícias particulares, porém conhecidas de forma legítima pelo divulgador.

Essa tentativa de diferenciar a privacidade, também chamada de vida privada, da intimidade seria, na opinião de Rodríguez[424], uma questão mais inerente ao campo linguístico, o que não significa que não há distinção entre os significados das duas palavras. É possível que existam informações que pertençam à vida privada do indivíduo que não sejam necessariamente íntimos.

O fato de não haver entendimento pacífico na doutrina sobre a existência de uma distinção entre os conceitos de direito à intimidade e direito à privacidade teve como resultado a criação de algumas correntes de pensamento[425]. Enquanto uma corrente acredita que não há qualquer diferença, sendo ambos decorrentes do direito da personalidade, outra defende que existe distinção entre o direito à intimidade e o direito à privacidade, sendo o primeiro, referente a um âmbito mais íntimo da vida humana, mais restrito que o segundo. Existe também uma terceira corrente doutrinária que acredita que o direito à intimidade engloba outros que derivam dele, inclusive o direito à vida privada. Dessa maneira, o direito à intimidade abrange outros como o direito à imagem, à inviolabilidade do domicílio e à produção artística e literária

Malgrado haja esses esforços no sentido de distinguir os termos retromencionados, existe um consenso no que tange ao status do direito à intimidade e do direito à privacidade como inerentes a todo e qualquer ser humano, o que os torna direitos da personalidade[426]. São direitos que podem ser exercidos inclusive frente ao Estado, só podendo ser restritos em situações excepcionais e se houver previsão nesse sentido na legislação.

Devido ao grau de dependência que boa parte da população mundial apresenta em relação aos dispositivos de comunicação pessoal, que armazenam informações sobre os aspectos financeiros, profissionais e pessoais da vida dos seus respectivos titulares, é possível considerar que os sistemas informáticos são sigilosos, bem como alguns dados particulares[427].

---

[424] *Ibidem, loc. cit.*
[425] CARVALHO, Luis Gustavo Grandinetti Castanho de. Direito à privacidade. **Revista da EMERJ**. Rio de Janeiro, v. 1, n. 2, 1998, p. 52.
[426] SILVA, César Dario Mariano da. **Tutela Penal da Intimidade**. Curitiba: Juruá. 2015, p. 56.
[427] SYDOW, Spencer Toth; CASTRO, Ana Lara Camargo de. *Op. cit*., p. 92.

Somente o usuário da conta do sistema ou a pessoa que criou os dados possui autorização para ter o acesso ao conteúdo que lhe diz respeito e apenas ele pode estendê-lo a terceiros, o que é chamado por Sydow e Castro[428] de confidencialidade informática. Além disso, os autores elucidam que a ninguém é permitido, além do próprio titular, modificar arquivos ou sistemas, a menos que haja autorização do mesmo nesse sentido. Trata-se da integridade informática. Por fim, a disponibilidade informática consiste no fato de que o usuário deve ter acesso aos seus dados e contas em redes sociais, bancos e nuvens quando bem entender e precisar.

Esses três componentes formam um novo bem jurídico denominado segurança informática ou segurança telemática[429]. Nesse trabalho defende-se a concepção de que a segurança telemática pode ser considerada como um desdobramento do direito à intimidade, mais abrangente do que o direito à intimidade, mesmo porque, conforme destacam Sydow e Castro[430], há condutas no ambiente cibernético que repercutem no espaço "real" e vice-versa.

Na subseção seguinte será explicada qual a trajetória histórica que a concepção acerca da intimidade percorreu e como foi elevada à categoria de direito fundamental.

5.1 HISTÓRICO DOS DIREITOS FUNDAMENTAIS À INTIMIDADE E À PRIVACIDADADE

Ainda que haja uma crescente preocupação sobre o direito à intimidade e à vida privada na era da Internet, tais valores são considerados um objeto de inquietação sob perspectiva jurídica desde a antiguidade. Durães, Leão Junior e Sanches[431] explicam que, na Grécia Antiga, a vida humana era dividida em dois âmbitos: a vida pública e a vida privada. Enquanto a vida pública consistia na participação do cidadão na polis, a vida privada restringia-se ao lar. Dessa forma, percebe-se que há uma preocupação em distinguir esses setores da vida da pessoa, ainda que na época tal entendimento fosse relativo apenas aos homens.

Durante a época dos romanos, considera-se que foi estabelecido um conceito mais preciso do que seria a intimidade, segundo leciona Herrán Ortiz citada por Rodríguez[432]. Esse povo

[428] *Ibidem*, p. 92-93.
[429] *Ibidem*, p. 93.
[430] *Ibidem*, p. 94.
[431] DURÃES, Cintya Nishimura; LEÃO JUNIOR, Teofilo Marcelo de Area; SANCHES, Raquel Cristina Ferraroni. Tutela do Direito à Intimidade. **Revista Eletrônica de Graduação do UNIVEM [REGRAD]**. Marília, 2014, n. 1, p. 76.
[432] HERRÁN ORITZ, Ana Isabel, **La violacion de la intimidad en laproteccion de datos personales**. Madri:

considerava que havia um "direito à propriedade do eu" expressado pela máxima do respeito ao próximo. Contudo, decisões judiciais da Roma Antiga buscadas pela autora demonstram o descaso com a intimidade alheia, como a declaração de ilegalidade de enlaces entre indivíduos considerados idosos, por entender que a união não apresentava utilidade. Destaca-se que também houve precedentes nos quais se garantiu a proteção jurídica da correspondência e do domicílio.

Com o advento do Cristianismo, as pessoas sentiram necessidade de passar períodos em retiro para orar e refletir, de modo que o recolhimento adquiriu uma faceta espiritual[433]. Isso se deve ao fato de que, supostamente, era mais provável que Deus se manifestasse nos momentos em que as pessoas estivessem recolhidas. O próprio catolicismo trouxe a valorização da privacidade e da intimidade com o sacramento da confissão, durante o qual as informações partilhadas entre o adepto da religião e o padre deveriam ser preservadas. Entretanto, é preciso ressaltar que, durante a Alta Idade Média, as poucas pessoas que dispunham de um espaço de fato reservado eram os membros de ordem religiosa, como os monges que ficavam recolhidos em monastérios[434].

Nesse período da Idade Média, houve três fatores determinantes para que o conceito de intimidade fosse aprimorado: a continuidade da intervenção do pensamento romano; o avanço da cultura germânica; a ideologia cristã[435]. O pensamento de São Tomás de Aquino sobre o tema consiste na concepção de que o homem é dotado de bens externos, como a propriedade e internos, como a intimidade. Essa última seria efeito do reconhecimento de cada pessoa como única e possuidora de um conjunto de valores e experiências.

A Igreja Católica, durante a época da Inquisição, conseguiu reunir um acervo com informações detalhadas sobre orientação sexual, intelectual, condições de saúde e dados sobre a ascendência e descendência dos indivíduos[436]. Esses registros tinham por objetivo facilitar o trabalho de persecução dos tribunais inquisitoriais. Após algum tempo, esses procedimentos

---

Dykinson, 1998, p. 4 apud RODRÍGUEZ, Víctor Gabriel. *Op. cit.*, p. 10.

[433] RODRÍGUEZ, Víctor Gabriel. *Op. cit*., p. 10.

[434] MEDRANO, Marcia Muñoz de Alba. La protección de la persona frente a las tecnologías de la comunicación. In: SALGADO, David Cienfuegos; VÁZQUEZ, Maria Carmen Macías (Coords.). **Estudios em homenaje a Marcia Muñoz de Alba Medrano**. Cidade do México: Universidad Autónoma del México, 2006, p. 3.

[435] HERRÁN ORITZ, Ana Isabel, **La violacion de la intimidad en laproteccion de datos personales**. Madri: Dykinson, 1998, p. 7 apud RODRÍGUEZ, Víctor Gabriel. *Op. cit.*, p. 11.

[436] PINO, Martim Manuel; GONÇALVES, Diego Marques. Os direitos à intimidade e à privacidade em face aos mecanismos de coleta de dados pessoais na rede mundial de computadores. **Revista de Propriedade Intelectual, Direito Contemporâneo e Constituição**. Aracaju, 2017, v. 11, n. 03, p. 4.

foram adotados pelas autoridades estatais para que pudessem exercer um controle mais efetivo sobre as pessoas.

Com o processo de urbanização desenvolvido na Baixa Idade Média, decorrente do aprimoramento das técnicas de manufatura e da divisão do trabalho, o entendimento acerca da noção de intimidade sofreu modificações[437]. Ao ser organizarem em cidades, as pessoas começaram a reivindicar certo espaço de caráter exclusivo, sem a interferência de terceiros.

Um exemplo dessas mudanças pode ser percebido na Inglaterra, onde desde o século XVI havia menção à inviolabilidade do domicílio, o que é expresso na máxima "*a man´s house is his castle*" (a casa de um homem é seu castelo). A proteção do domicílio, contudo, não chegava a abranger outras formas de privacidade, como a privacidade das comunicações e informações[438]. A tutela desses direitos só foi discutida no século XIX, quando essas formas de privacidade começaram a ser consideradas direitos autônomos.

É preciso salientar que a organização da sociedade europeia era desfavorável à existência do individualismo, situação que perdurou, mais especificamente, até o século XVIII[439]. A primazia sobre a noção do coletivo impedia que se desenvolvesse uma tutela da vida privada, conjuntura alterada com o advento da Revolução Francesa. Tal acontecimento trouxe novos valores, de modo que os costumes burgueses passaram a ser compreendidos como um sistema de referência, tendo a intimidade e a vida privada como elementos relevantes para um indivíduo.

Assim, considera-se que o direito à vida privada e o direito à intimidade são duas conquistas do pensamento liberal vigente nos séculos XVII e XVIII, conforme destacam Ávila e Woloszyn[440]. Tais direitos relacionam-se ao âmbito das liberdades individuais, de modo que, progressivamente, começaram a ser previstos nas constituições de diversos países, bem como vários documentos que versam sobre a proteção dos direitos humanos foram elaborados nos séculos seguintes.

---

[437] MEDRANO, Marcia Muñoz de Alba. *Op. cit.*, p. 3.
[438] PINO, Martim Manuel; GONÇALVES, Diego Marques. *Op. cit.*, p. 5.
[439] ZANINI, Leonardo Estevam de Assis. A proteção da imagem e da vida privada na França. **Revista Brasileira de Direito Civil**, Belo Horizonte, 2018, v. 16, p. 58.
[440] ÁVILA, Ana Paula Oliveira; WOLOSZYN, André Luis. A tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência. **Revista de Investigações Constitucionais**. Curitiba, 2017, v. 4, n. 3, p. 171.

Ressalte-se que o desenvolvimento do direito à intimidade correspondeu, no aspecto prático inicialmente, ao reconhecimento de uma regalia de certa classe social, no caso, a burguesia[441]. Apesar de a tutela desses valores ter sido, gradativamente, reconhecida pela comunidade internacional como uma proteção inerente a todos os seres humanos, a essência desses é considerada um aspecto ideológico próprio da referida classe social.

Um dos primeiros registros da judicialização da salvaguarda da intimidade ocorreu na França, em um julgado do Tribunal Cível do Sena, em 1858[442]. A situação envolveu a irmã de um artista, que designou dois pintores para retratá-la em seu leito de morte. Ocorre que o quadro foi exposto e colocado à venda sem autorização, o que acarretou na decisão do Tribunal de confiscar a pintura, bem como seus registros fotográficos. A corte foi favorável ao entendimento de que a pessoa teria o direito de usufruir de sua vida privada, ainda que em ocasião de seu óbito, de forma que o registro desse momento não poderia ser exposto.

Nos Estados Unidos tal direito ganhou notoriedade a partir de 1891 com um artigo publicado por Samuel Warren e Louis Brandeis[443]. Foi utilizado como arcabouço teórico a obra de um magistrado chamado Thomas Cooley publicada em 1873, conforme o sistema *common law*, bem como estudos sobe o direito à solidão. Os autores tinham como intuito garantir que a alta burguesia da época não tivesse sua intimidade violada principalmente pela imprensa. A situação que deu ensejo a esse trabalho de Warren e Brandeis será explanada mais adiante.

A tutela da intimidade nos Estados Unidos foi prevista na Lei dos Direitos Civis de Nova York[444] em 1903. Tal legislação dispunha sobre sanções em caso de utilização, com intuito comercial ou publicitário, do nome, retrato ou desenho alheio sem o consentimento. A conduta em questão, de acordo com a lei, poderia ser cometida por uma pessoa física ou jurídica.

Já na Europa continental, a proteção da intimidade só foi intensificada em meados do século XX, por conta das ameaças que vinham ocorrendo em um contexto de vigilância e controle

---

[441] MAIA, Luciano Soares. A privacidade e os princípios de proteção do indivíduo perante os bancos de dados pessoais. In: Conselho Nacional de Pesquisa e Pós- Graduação em Direito (CONPEDI). **Anais do XVI Congresso Nacional do Conpedi**. Florianópolis: Fundação Boiteux, 2008, p. 455.
[442] COSTA JÚNIOR, Paulo José da. *Op. cit.*, p. 15.
[443] DURÃES, Cintya Nishimura; LEÃO JUNIOR, Teofilo Marcelo de Area; SANCHES, Raquel Cristina Ferraroni. *Op. cit*., p. 76.
[444] ESTADOS UNIDOS. New York Civil Rights Law, abr.1903, **Laws of the State of New York Passed at the Sessions of the Legislature**, vol. 01, 1903. Disponível em: https://babel.hathitrust.org/cgi/pt?id=nyp.33433090742549&view=1up&seq=320. Acesso em: 09 mar. 2020.

das pessoas por meio da coleta de informações[445]. Durante o período da Guerra Fria surgiram as primeiras expressões do emprego da tecnologia para obter e armazenar informações pessoais.

No final da década de 1950, Heinrich Henkel propôs durante o *Deutscher Juristentag* (Fórum Jurídico Alemão) a teoria das três camadas, também conhecida como teoria dos círculos concêntricos[446]. O círculo da vida privada em sentido estrito seria composto por informações pessoais que apresentam caráter público, tais como endereço e telefone. Após esse círculo haveria a camada da intimidade, que engloba informações confidenciais compartilhadas com familiares, amigos, colegas do âmbito profissional. Por último, o círculo do segredo ou nuclear incluiria as informações mais íntimas do ser humano.

Apesar de ser um assunto que vem se mostrando objeto de intenso interesse por parte dos juristas do mundo inteiro desde o século XIX e da menção ao direito à intimidade na legislação de diversos países, faz-se relevante destacar que a comunidade internacional já havia realizado um debate sobre o assunto na década de 1940.

A Declaração Universal dos Direitos Humanos[447], documento proclamado pela Assembleia Geral das Nações Unidas em 1948 e considerada um marco na história dos direitos humanos, estabelece em seu art. 12 que "ninguém deverá ser submetido a interferências arbitrárias na sua vida privada, família, domicílio ou correspondência, nem a ataques à sua honra e reputação". Ademais, o texto do documento afirma que "contra tais intromissões ou ataques todas as pessoas têm o direito à proteção da lei". Tal menção reforça o compromisso dos Estados signatários nesse sentido.

Na década de 1960 também houve a elaboração de documentos internacionais nesse sentido, como o Pacto Internacional de Direitos Civis e Políticos[448] (1966), que atesta em seu art. 17 que a privacidade dos indivíduos deve ser objeto de salvaguarda:

> Ninguém poderá ser objeto de ingerências arbitrárias ou legais em sua vida privada, em sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais

[445] MAIA, Luciano Soares. *Op. cit*., p. 455-456.
[446] PINO, Martim Manuel; GONÇALVES, Diego Marques. *Op. cit.*, p 8-9.
[447] ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. Paris, 1948. Disponível em: https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por. Acesso em: 20 set. 2019.
[448] ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS. **Pacto Internacional sobre Direitos Civis e Políticos**. Nova Iorque, 1966. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm. Acesso em: 20 set. 2019.

> à sua honra e reputação. Toda pessoa terá direito à proteção da lei contra essas ingerências ou ofensas.

Percebe-se que a preocupação da comunidade internacional sobre o assunto continuou sendo relevante durante os debates sobre a proteção aos direitos humanos.

Faz-se relevante destacar também a Conferência Nórdica sobre Direito à Intimidade, realizada em maio de 1967 na cidade de Estocolmo, na qual se conceituou a intimidade como o direito do ser humano de viver sua vida de maneira independente, com reduzida interferência alheia[449]. Durante esse evento houve foco exclusivo no tema, destacando a necessidade de proteger a intimidade do indivíduo contra as seguintes interferências: acúmulo não autorizado de registros sobre a pessoa; gravação de som e registros fotográficos ou cinematográficos; importunamentos pela imprensa ou meios de comunicação em massa; fustigamento de pessoa, o que consiste em acossar, observar ou expor conteúdos de chamadas telefônicas[450].

No âmbito dos sistemas internacionais de proteção aos direitos humanos, que são o conjunto de normas, órgãos e mecanismos que têm por finalidade proporcionar a salvaguarda desses direitos[451], também está prevista a tutela da intimidade. Além do sistema universal dos direitos humanos, proveniente da já mencionada Declaração Universal dos Direitos Humanos, há três sistemas de proteção: europeu, interamericano e africano.

A Convenção Europeia de Direitos Humanos[452] foi adotada pelo Conselho da Europa em 4 de novembro de 1950, tendo entrado em vigor três anos depois. Como a noção de dignidade da pessoa humana está intrinsecamente ligada à questão da salvaguarda da intimidade, o assunto também está previsto nesse tratado, mais especificamente em seu art. 8º:

> Artigo 8° Direito ao respeito pela vida privada e familiar
> 1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.
> 2. Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem - estar económico do país, a defesa da ordem e a

[449] CASTRO, Leonardo Bellini de. As Implicações Jurídico-Constitucionais da Tutela da Intimidade e suas Relações com a Atividade Investigatória do Estado. **Revista Jurídica ESMP-SP**. São Paulo, v. 4, 2013, p. 63.
[450] CORDEIRO, Edmar Lima. Direito à Privacidade de Informação. **Revista de Ciências Jurídicas e Sociais da UNOPAR**. Toledo, 2001 v. 4, p. 12.
[451] BRASIL. Sistemas Internacionais de Proteção aos Direitos Humanos: Apresentação. **Ministério Público Federal.** Disponível em: http://midia.pgr.mpf.mp.br/pfdc/hotsites/sistema_protecao_direitos_humanos/index.html. Acesso em: 14 mar. 2020.
[452] CONSELHO DA EUROPA. **Convenção Europeia dos Direitos Humanos**. Roma, 4 de novembro de 1950. Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf. Acesso em: 14 mar. 2020.

> prevenção das infracções penais, a protecção da saúde ou da moral, ou a protecção dos direitos e das liberdades de terceiros.

O Conselho da Europa, fundado em 1949, é a principal organização para defender os direitos humanos no continente[453]. A organização possui em seu quadro de colaboradores um grupo de constitucionalistas denominado Comissão de Veneza, que é responsável pelas orientações jurídicas disponibilizadas para os países. O Conselho incluiu na Convenção Europeia o art. 8º em correspondência ao art. 12 da Declaração Universal dos Direitos Humanos por admitir a importância do direito à reserva da vida privada, familiar, doméstica e sentimental, que se torna cada vez mais um objeto de preocupação no atual contexto social[454].

Já houve um precedente que demandou um posicionamento do Tribunal Europeu de Direitos Humanos (TEDH) em caso de colisão entre o direito à vida privada e a questão do interesse público. A polícia da Eslovênia, durante uma operação que investigava a difusão de material pornográfico infantil, requisitou a uma empresa provedora de Internet, sem a autorização de uma ordem judicial, nomes e números de IPs de usuários suspeitos[455]. Posteriormente, um juiz emitiu uma ordem demandando o mesmo da empresa e autorizando os policiais a realizarem buscas nos domicílios dos investigados.

Durante a busca e apreensão foram apreendidos quatro computadores e, após a perícia, foi constatado que o material pertencia ao filho de um dos contratantes do serviço de Internet[456]. Ele foi processado e condenado pelo crime de posse e distribuição de conteúdo pornográfico infantil e recorreu alegando que as informações disponibilizadas pela empresa foram obtidas sem autorização judicial. Contudo, a sentença da primeira instância foi mantida nas instâncias superiores e no TEDH, que determinou apenas que a Eslovênia indenizasse o demandante.

Outro sistema regional que também prevê a salvaguarda do direito à intimidade é o sistema interamericano de direitos humanos. Esse é o sistema que se aplica ao Brasil e é composto pela Comissão Interamericana de Direitos Humanos e pela Corte Interamericana de Direitos

---

[453] *Idem*. **Valores: Direitos Humanos, Democracia, Estado de Direito**. Disponível em: https://www.coe.int/pt/web/about-us/values. Acesso em: 14 mar. 2020.

[454] LEÃO, Anabela Costa; NEVES, Inês; COUTINHO, Juliana Ferraz; NETO, Luísa (Coords.). **Declaração Universal dos Direitos Humanos | Convenção Europeia dos Direitos Humanos: Anotações pelos estudantes da Faculdade de Direito da Universidade do Porto**. Porto: Universidade do Porto, 2019, p. 88.

[455] TRIBUNAL EUROPEU DE DIREITOS HUMANOS. **Case of Benedik v. Slovenia (Application no. 62357/14)**. Estrasburgo, 24 jul. 2018. Disponível em: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-182455%22]}. Acesso em: 17 mar. 2020.

[456] *Idem*. Disponível em: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-182455%22]}. Acesso em: 17 mar. 2020.

Humanos, ambos órgãos de monitoramento pertencentes à Organização dos Estados Americanos (OEA)[457]. De acordo com informações do próprio site da OEA, trata-se do organismo regional mais antigo do mundo, tendo suas origens na Primeira Conferência Internacional Americana, realizada em Washington, capital dos Estados Unidos, de outubro de 1889 a abril de 1890[458].

A OEA possui alguns documentos que regem o sistema interamericano de direitos humanos, sendo um dos mais relevantes a Convenção Americana de Direitos Humanos[459], também chamada de Pacto de San José da Costa Rica, um tratado internacional celebrado no ano de 1969 pelos países-membros da OEA. No art. 11 está prevista a proteção da honra e da dignidade, direitos inerentes a todas as pessoas, e também está disposto que ninguém pode ser objeto de interferência arbitrária ou abusiva no âmbito de sua vida privada ou nas vidas de membros de sua família, bem como em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação. Contudo, é preciso ressaltar que no item 2 do art. 32 está disposto que que os direitos individuais são limitados pelos direitos dos demais, por conta da segurança geral e pelas justas exigências do bem da coletividade em uma sociedade democrática.

Assim como o TEDH, a Corte Interamericana de Direitos Humanos (CIDH) também já enfrentou uma situação de colisão entre direitos. O conflito em questão entre o direito à intimidade e o direito à liberdade de expressão. Em 1995, uma revista argentina dirigida pelos editores Jorge Fontevecchia e Hector D'Amico publicou uma matéria sobre um suposto filho do então presidente do país, Carlos Saúl Menem[460].

Menem entrou com uma ação demandando um ressarcimento por violação à intimidade e que a sentença condenando os editores, o que não foi acatado pela primeira instância[461]. Recorreu,

---

[457] BRASIL. Sistemas Internacionais de Proteção aos Direitos Humanos: Apresentação. **Ministério Público Federal.** Disponível em: http://midia.pgr.mpf.mp.br/pfdc/hotsites/sistema_protecao_direitos_humanos/index.html. Acesso em: 14 mar. 2020.

[458] ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Quem Somos**. Disponível em: http://www.oas.org/pt/sobre/quem_somos.asp. Acesso em: 14 mar. 2020.

[459] COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS. **Convenção americana sobre direitos humanos**. Disponível em: https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm. Acesso em: 20 set. 2019.

[460] CORTE INTERAMERICANA DE DIREITOS HUMANOS. **Fontevecchia y D'amico Vs. Argentina**. Washington, 29 nov. 2011. Disponível em: http://www.corteidh.or.cr/CF/jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=191. Acesso em: 17 mar. 2020.

[461] *Idem*. Disponível em: http://www.corteidh.or.cr/CF/jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=191. Acesso em: 17 mar. 2020.

então, à Câmara Nacional de Apelações reverteu a decisão e condenou Fontevecchia e D'Amico ao pagamento de indenização. O caso chegou à CIDH, que considerou que a revista tratava de assuntos de interesse público e, sendo Menem um alto funcionário do governo argentino, a notícia em questão era admissível, de modo que a imposição de medidas sancionatórias aos jornalistas violaria o direito à liberdade de expressão.

Existe ainda o sistema africano de proteção aos direitos humanos, o mais recente de todos. A Carta Africana dos Direitos Humanos e dos Povos[462], também chamada de Carta de Banjul, foi aprovada em 1981, mas, diferente das outras convenções sobre direitos humanos, ela não tem previsão expressa sobre a proteção da intimidade ou da privacidade.

Para compreender o motivo pelo qual não incluiu expressamente esse direito na Carta de Banjul, Pedro Rosa Có[463] explica que o "compromisso de evolução coletiva" previsto no tratado consiste em um acordo entre os Estados africanos para concretizar as normas previstas no documento e completá-lo, se necessário, por meio de instrumentos oficiais. Dentre os fatores que levaram à omissão de certos direitos, como a proteção à privacidade, está a conjuntura na qual foi elaborada o documento, optando-se por uma linguagem mais abrangente, para que outros direitos fossem inclusos posteriormente.

Com a exposição desses fatos, pode-se considerar que o direito à privacidade é tratado como um direito amplo, sendo que alguns ordenamentos jurídicos consideram a expressão sinônima do termo "direito à intimidade" ou como um direito que engloba a proteção à intimidade. Dessa forma, a proteção da privacidade é mencionada com mais frequência nos ordenamentos jurídicos dos Estados em geral

Ademais, esse direito é salvaguardado em diversos países e em sistemas de proteção aos direitos humanos. Na subseção seguinte serão explanados precedentes e normas voltados à proteção do direito à intimidade em alguns Estados.

5.2 PRECEDENTES E NORMAS ESTRANGEIROS SOBRE A MATÉRIA

[462] ORGANIZAÇÃO DA UNIDADE AFRICANA. **Carta Africana dos Direitos Humanos e dos Povos**. Banjul, jan. 1981. Disponível em: http://www.dhnet.org.br/direitos/sip/africa/banjul.htm. Acesso em: 14 mar. 2020.

[463] CÓ, Pedro Rosa. Artigo 66: Protocolos ou acordos particulares poderão completar, em caso de necessidade, as disposições da presente Carta. In: JERÓNIMO, Patrícia; GARRIDO, Rui; PEREIRA, Maria de Assunção do Vale. **Comentário Lusófono à Carta Africana dos Direitos Humanos e dos Povos**. Braga: Observatório Lusófono dos Direitos Humanos da Universidade do Minho (OLDHUM), 2018, p. 535.

Um dos países no qual mais se desenvolveu estudos sobre o direito à intimidade foram os Estados Unidos. O termo utilizado no país é "*right to privacy*", que, em tradução direta para a língua portuguesa significaria "direito à privacidade", porém a legislação do país não especifica a diferença entre privacidade e intimidade, apenas destaca que a privacidade é um direito tutelado[464]. Há precedentes sobre a proteção do direito à privacidade, principalmente após a Quarta Emenda à Constituição estadunidense[465], introduzida em 1791, que versa sobe a proibição de buscas e apreensões arbitrárias.

Para os estadunidenses, a privacidade seria decorrente do direito à propriedade, de forma que o poder estatal não poderia invadir, controlar ou dispor da propriedade de particulares, a não ser que haja motivos relevantes o suficiente para ensejar tais ações[466]. Atualmente, contudo, a compreensão do direito é mais abrangente, por conta do aumento do nível de complexidade do cenário social.

Um dos casos emblemáticos que levou a doutrina estadunidense a refletir sobre a dimensão do direito à intimidade, e que influenciou juristas de vários países, envolveu uma atriz, o que remete à situação de exposição desautorizada que o gênero feminino enfrenta até os dias de hoje, quando imagens de mulheres em cenas íntimas são compartilhadas na Internet sem seu consentimento. No final do século XIX, a atriz Marion Manola estava atuando em uma peça de teatro na Broadway e, em uma das cenas em que aparecia no palco apenas usando roupas íntimas, foi fotografada sem sua autorização[467].

Antes desse fato ocorrer, a companhia de teatro propôs que a fotografia fosse tirada para ser utilizada em anúncios da peça que estava em cartaz. Entretanto, Manola não aceitou a proposta por alguns fatores. Para a atriz, suas habilidades de canto e atuação deveriam ser mais valorizadas do que a exposição da sua imagem em anúncios. Além disso, Marion Manola tinha uma filha que era criança na época e não se sentia confortável com a ideia de a

---

[464] GARCIA, Rafael de Deus. Os direitos à privacidade e à intimidade: origem, distinção e dimensões. **Revista da Faculdade de Direito do Sul de Minas**. Pouso Alegre, 2018 v. 34, p. 6.
[465] ESTADOS UNIDOS. Quarta Emenda à Constituição. **United States Courts**. Disponível em: https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0. Acesso em: 07 mar. 2020.
[466] GARCIA, Rafael de Deus. *Op. cit*., p. 6.
[467] GLANCY, Dorothy J. Privacy and the Other Miss M. **Santa Clara Law Digital Commons**. Santa Clara, 1989/1990, n. 10, p. 414.

menina perceber uma foto de sua mãe em trajes íntimos estava exposta em jornais e revistas[468].

A atriz recorreu à justiça dos Estados Unidos para assegurar seu direito à imagem, o que foi considerado pelos empresários da companhia teatral como uma oportunidade de atrair mais público para a peça. Enquanto mulheres escreveram cartas apoiando o posicionamento de Manola, a maior parte das pessoas não deu muita importância à situação, pois era normal que atrizes aparecessem em trajes íntimos em público[469].

Percebe-se nessa conjuntura mais uma manifestação do machismo, sendo a exposição da imagem do corpo da mulher era considerada uma questão irrelevante, pois tratava-se de uma pessoa acostumada com esse tipo de exibição. Uma situação parecida ocorreu em 2018 com Paolla Oliveira, que teve fotos divulgadas na Internet obtidas clandestinamente enquanto ela gravava cenas para uma minissérie[470]. Mesmo com mais de cem anos separando o caso da atriz estadunidense e o da brasileira, as violações do direito à intimidade da mulher ainda são frequentes, ainda que sejam pessoas públicas.

O caso de Marion Manola chamou a atenção dos advogados Louis Brandeis e Samuel Warren, que escreveram um artigo denominado *The Right to Privacy* na *Harvard Law Review* em 1890[471]. Os autores defenderam no trabalho a tese de que o sistema *common law* assegura o direito individual de compartilhar o que a pessoa entender que deve com os outros, sendo o meio adotado para expressar tais informações irrelevante. Assim, pode-se alegar um princípio semelhante para evitar a exposição desautorizada de uma pessoa com meios como a fotografia ou qualquer outro que permita o registro de imagens.

Havia, antes da tese defendida por Brandeis e Warren, uma ampla variedade de conceitos legais e precedentes no sistema *common law* sobre a proteção desse bem jurídico[472]. O mérito dos autores se deve ao fato de que eles organizaram essas concepções que permeavam a *common law* para chegar ao princípio jurídico do direito à privacidade. O trabalho dos

---

[468] *Ibidem*, p. 414-415.
[469] *Ibidem*, p. 415-416.
[470] PAOLLA Oliveira tem fotos íntimas vazadas. **Revista Cláudia**, 02 mar. 2018. Disponível em: https://claudia.abril.com.br/famosos/globo-descobre-responsavel-divulgacao-fotos-intimas-de-paolla-oliveira/. Acesso em: 10 mar. 2020.
[471] WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**. Cambridge, 1890, v. 4, n. 5, p. 193-220.
[472] GLANCY, Dorothy J. The Invention of the Right to Privacy. **Arizona Law Review**. Tucson, 1979, v. 21, n. 1, p. 3.

advogados estadunidenses deu contornos próprios a esse direito, por isso causou tanta repercussão à época.

Nos Estados Unidos, o direito à privacidade tem o status negativo, ou seja, as pessoas não devem se submeter a investigações invasivas por parte do Estado, não há um dever constitucional direcionado ao Estado de proteger o âmbito particular da existência do indivíduo[473]. Para salvaguardar esse bem jurídico no ciberespaço, o país conta com um órgão público denominado *Department of Homeland Security* (Departamento de Segurança Interna)[474] para estabelecer políticas públicas nesse sentido e fiscalizar o cumprimento das leis sobre a matéria.

Já na Alemanha, país onde foi elaborada uma das teorias sobre o direito à privacidade mais conhecidas, o direito à privacidade apresenta um status positivo, tendo o *Bundesverfassungsgericht*, órgão responsável pela interpretação da constituição, considerado que o Estado deve criar condições para que a esfera privada seja protegida[475].

A Constituição Alemã[476] (*Grundgesetz*), assim como a estadunidense, não apresenta um direito geral à privacidade. Os interesses privados do indivíduo estão previstos nos seguintes artigos da *Grundgesetz*: art. 1º, que versa sobre a inviolabilidade da dignidade humana; art. 2º, que trata sobre as liberdades pessoais, em seu item 1, segundo o qual toda pessoa tem o direito de desenvolver sua responsabilidade livremente; art. 10º, que aborda a privacidade das correspondências e das telecomunicações; art. 13, no qual está prevista a inviolabilidade do domicílio.

O capítulo 15 do código penal alemão[477] versa sobre violação da privacidade e da esfera pessoal, sendo os crimes nesse sentido previstos entre as seções 201 e 206. Dentre as condutas tipificadas na referida legislação estão a ofensa à intimidade por meio do registro de imagens (seção 201) e a violação do sigilo de correspondência enviada pelo correio ou de telecomunicações (seção 206). Em 2006, a legislação sofreu algumas mudanças, dentre as

[473] JACOBY, Nicole. Redefining the right to be let alone: privacy rights and the constitutionality of technical surveillance measures in germany and the united states. **Georgia Journal of International and Comparative Law**. Athens, 2007, v. 35, n. 3, p. 435.
[474] ESTADOS UNIDOS. **Cybersecurity and Privacy**. Departamento de Segurança Interna. Disponível em: https://www.dhs.gov/cybersecurity-and-privacy. Acesso em: 17 mar. 2020.
[475] *Idem*. Disponível em: https://www.dhs.gov/cybersecurity-and-privacy. Acesso em: 17 mar. 2020
[476] ALEMANHA, **Constituição da República Federal da Alemanha**. Bonn, 23 de maio de 1949. Disponível em: https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html. Acesso em: 15 mar. 2020.
[477] *Idem*. **Código Penal Alemão**, Berlin, 13 nov. 1998. Disponível em: https://www.gesetze-im-internet.de/stgb/. Acesso em: 16 mar. 2020.

quais houve a inclusão das seções 202 a, b, c e d. Essas normas são desdobramentos da seção 202, que versa sobre a violação à correspondência. Os crimes incluídos na legislação germânica foram: espionagem de dados (202a); *phishing* (202b); atos preparatórios para espionagem de dados ou *phishing* (202c); manipulação de dados roubados (202d).

Percebe-se que houve uma preocupação do legislador alemão em proteger os dados particulares no ambiente informático de ataques cibernéticos. Contudo, o país continua buscando aperfeiçoar seus mecanismos de combate à criminalidade informática, como ocorreu na operação realizada pela polícia alemã em conjunto com a *Europol* para identificar usuários do *malware DroidJack* em seu território[478]. O programa é utilizado para invadir dispositivos informáticos e, por conseguinte, acessar os dados dos seus titulares.

Outro país que também influenciou o entendimento de juristas brasileiros quanto ao direito à privacidade, conforme mencionado anteriormente, foi a Itália. Na constituição desse país, o direito à privacidade não está previsto de maneira expressa, porém encontra respaldo nos arts. 14 e 15, que versam, respectivamente, sobre a inviolabilidade do domicílio e sobre a garantia de sigilo de qualquer forma de comunicação[479].

Essas menções no texto constitucional da Itália fundamental a proteção de certos âmbitos da vida humana de interferências descabidas, conforme elucida Salerno[480]. Exemplos da proteção à privacidade e à intimidade podem ser encontrados nos arts. 621 e 623, nos quais se encontra proibição de revelar atos ou documentos alheios cujo conteúdo seja sigiloso e de tornar públicas informações secretas sobre descobertas e invenções científicas. Já o art. 622 tipifica a revelação de segredos profissionais sem justa causa.

Em 23 de dezembro de 1993 foi aprovada a Lei nº 547, que trata sobre delitos informáticos, modificando o código penal italiano. Essa norma incluiu o art. 615-ter, que criminaliza a conduta de acesso a um sistema informático protegido por sistema de segurança sem a autorização expressa ou tácita de quem dispõe do direito de excluí-lo. Foram adicionados também ao código penal o art. 615-quarter, que tipifica sobre a detenção e difusão abusiva de

[478] DAVIS, Jeremy Seth. German police coordinate with Europol to nab DroidJack useres. **SC Magazine**, 30 out. 2015. Disponível em: https://www.scmagazine.com/home/security-news/german-police-coordinate-with-europol-to-nab-droidjack-users/. Acesso em: 16 mar. 2020.

[479] ITÁLIA. **Constituição da República Italiana**. Roma, 22 dez. 1947. Disponível em: https://www.senato.it/documenti/repository/istituzione/costituzione.pdf. Acesso em: 16 mar. 2020.

[480] SALERNO, Giulio M. A Proteção da Privacidade e a Inviolabilidade da Correspondência. **Revista da AJURIS**, Porto Alegre, dez. 2012, v. 39, n. 128, p. 365.

códigos de acesso informáticos ou telemáticos, e o art. 615-quinquies, sobre a distribuição de programas com fins de danificar ou interromper o funcionamento de um sistema informático.

Na França, país onde surgiram as primeiras noções sobre o direito à privacidade, a violação a esse bem jurídico é prevista no código penal em seu capítulo IV, seção 1, nos arts. 226-1 ao 226-7 [481]. Ademais, o art. 323-1 prevê o crime de acesso fraudulento de dispositivo automatizado de tratamento de dados e o art. 323-3 criminaliza a introdução fraudulenta de dados em um sistema automatizado, bem como a extração, a extinção, a reprodução ou modificação desautorizada de dados.

Sobre o aumento de casos de implementação de mecanismos para fins de espionagem nos dispositivos informáticos, a Agência Nacional de Segurança de Sistemas da Informação (ANSSI) [482] disponibiliza notícias frequentes nesse sentido para particulares, funcionários públicos e integrantes de organizações empresariais. Em janeiro de 2020, a ANSSI participou do Fórum Internacional de Cibersegurança, evento no qual se definiram medidas internas e de cooperação internacional para garantir a estabilidade do ambiente cibernético[483].

As conjunturas retromencionadas são de países que já se preocupam com questões envolvendo os direitos à intimidade e à privacidade há muito tempo e continuam buscando formas de garantir esses direitos no ciberespaço. Na subseção seguinte será explicado como tais bens jurídicos são tratados na legislação do Brasil.

5.3 NORMAS DO ORDENAMENTO JURÍDICO BRASILEIRO

Os direitos à intimidade e à vida privada são, conforme mencionado anteriormente, objeto de proteção de diversos tratados, sendo que os Estados membros devem tomar providências necessárias nas legislações internas a fim de concretizar tal objetivo. No Brasil, Silva[484] destaca que não há entendimento harmonioso na doutrina se os conceitos de intimidade e vida privada são equivalentes ou apresentam distinções, pois, enquanto alguns autores consideram

[481] FRANÇA. **Código Penal Francês**. Paris, 01 março de 1994. Disponível em: https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719. Acesso em: 16 mar. 2020.
[482] FRANÇA. **Agence nationale de la sécurité des systèmes d'information**. Disponível em: https://www.ssi.gouv.fr/. Acesso em: 17 mar. 2020.
[483] *Idem*. FIC 2020: L´ANSSI plaide pour une souveranité européene en matiére de cybersecurité. **Agence nationale de la sécurité des systèmes d'information**. Disponível em: https://www.ssi.gouv.fr/actualite/fic-2020-lanssi-plaide-pour-une-souverainete-europeenne-en-matiere-de-cybersecurite/. Acesso em: 17 mar. 2020.
[484] SILVA, César Dario Mariano da. **Tutela Penal da Intimidade**. Curitiba: Juruá Editora, 2015, p. 22.

que ambos os termos se referem à mesma ideia, outros entendem que, com o advento da Constituição Federal de 1988, surgiram direitos autônomos.

No art. 5º, inciso X, da Constituição Federal de 1988[485] está previsto que a intimidade, a vida privada, a honra e a imagem das pessoas são direitos invioláveis, sendo cabível a indenização por dano material ou moral em caso de ofensa a esses direitos. O artigo em questão está localizado no Capítulo I (Dos Direitos e Deveres Individuais e Coletivos), que integra o Título II (Dos Direitos e Garantias Fundamentais), sendo considerado pela Carta Magna brasileira uma cláusula pétrea, o que assegura sua proteção no ordenamento jurídico do país.

Há direitos que visam salvaguardar o âmbito individual e outros tutelam a personalidade na esfera que constitui a vida pública. No campo individual estão o direito ao nome e o direito à reputação; o primeiro tutela a individualidade da pessoa contra violações por parte de terceiros, enquanto que o segundo protege o indivíduo contra atos difamatórios que maculam sua reputação social[486]. Na tutela da vida privada, por sua vez, trata-se da personalidade do cidadão em sua própria individualidade. Dessa forma, conclui-se que a esfera individual tutela o nome e a honra, enquanto a esfera privada protege o ser humano contra a indiscrição.

Para Silva[487], se o legislador constitucional diferenciou o conceito de intimidade do conceito de vida privada, não é razoável que a doutrina e a jurisprudência considerem que os dois termos versem sobre o mesmo assunto. A intimidade abrange informações sobre circunstâncias que, se forem divulgadas, podem causar danos morais ou materiais para seu titular. Já a noção de vida privada é composta por fatos que não são tão íntimos, ou seja, seria uma esfera menos reservada, mas que ainda assim poderia causar prejuízos ao titular em caso de exposição.

No Código Civil[488] brasileiro também é possível encontrar referência à proteção da vida privada em seu art. 21, de acordo com o qual o direito à vida privada não pode ser ofendido e que o interessado, em caso de violação desse direito, pode requerer ao juiz que sejam tomadas as medidas necessárias para proibir ou interromper ato contrário a essa norma.

---

[485] BRASIL. **Constituição da República Federativa do Brasil**. Brasília, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 20 set. 2019.
[486] SILVA, César Dario Mariano da. *Op. cit.*, p. 23.
[487] *Ibidem*, p. 27.
[488] BRASIL. **Lei nº 10.406**, de 10 de janeiro de 2002. Institui o Código Civil. Brasília, DF, 10 jan. 2002. Disponível em http://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406.htm. Acesso em: 20 mar. 2019.

Como nesse trabalho trata-se da proteção penal da intimidade, faz-se necessário ressaltar que, ainda que haja previsão constitucional acerca da inviolabilidade da vida privada e da intimidade, o atual Código Penal[489] brasileiro não apresenta previsão normativa de um tipo penal específico para evitar a ofensa a tais bens jurídicos. Dessa forma, o Direito Penal protege esses bens de maneira indireta, ou seja, criminaliza algumas práticas, tais como a violação de domicílio, das comunicações, de dispositivos informáticos e a revelação de algumas espécies de segredo.

Talvez um dos mais conhecidos tipos penais nesse sentido seja a violação de domicílio, previsto no art. 150 do Código Penal[490]. A casa é considerada asilo inviolável da pessoa humana, de forma que não se pode entrar na residência sem a anuência do morador, a não ser em situações que configurem flagrante delito, desastre, ou para prestação de socorro ou, durante o dia, por determinação judicial, conforme o art. 5º, inciso XI, da Constituição Federal. Dessa maneira, é compreensível que o legislador tenha criado esse tipo penal com a finalidade de proteger o reduto mais íntimo do indivíduo. Ressalte-se que no Código Penal de 1969, que nunca chegou a entrar em vigor, havia um tipo penal similar previsto no art. 159[491].

Como "casa", o §4º do art. 150 abrange: I – qualquer compartimento habitado; II – aposento ocupado de habitação coletiva; III – compartimento não aberto ao público onde alguém exerce profissão ou atividade. Silva[492] destaca que, para que ocorra o crime de violação de domicílio, a invasão da casa deve ser física, não havendo punição para invasão virtual. Em outras palavras, se um hacker conseguir invadir um sistema de automação da casa[493] ou mesmo o sistema de vigilância, acessando as câmeras da residência, não poderá ser punido penalmente, pois a lei não prevê essa possibilidade de invasão de domicílio.

Acerca do sigilo, Ávila e Wolozyn[494] explicam que segredo é algo que não pode e nem deve vir a público. O sigilo de cartas e documentos consiste na não-violação da correspondência por funcionários dos correios ou terceiros. É possível ampliar esse conceito para incluir dados

---

[489] SILVA, César Dario Mariano da. *Op. cit*., p. 23.
[490] BRASIL. **Decreto-lei nº 2.848**, de 7 de dezembro de 1940. Código Penal. Brasília, DF, 7 dez. 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm. Acesso em: 20 mar. 2020.
[491] *Idem*. **Decreto-lei nº 1.004**, de 21 de outubro de 1969. Código Penal. Brasília, DF, 21 out. 1969. Disponível em: http://www.planalto.gov.br/ccivil_03/Decreto-Lei/1965-1988/Del1004.htm. Acesso em: 20 mar. 2020.
[492]SILVA, César Dario Mariano da. *Op. cit.*, p. 134.
[493] A automação residencial é a associação de vários equipamentos motorizados e automatizados que mantém contato entre si. Para mais informações ver: SMAAL, Beatriz. **Automação residencial: a tecnologia invade a sua casa.** Disponível em: https://www.tecmundo.com.br/casas/9907-automacao-residencial-a-tecnologia-invade-a-sua-casa.htm. Acesso em: 20 set. 2019.
[494] ÁVILA, Ana Paula Oliveira; WOLOSZYN, André Luis. *Op. cit*., p. 176.

e comunicações que ocorrem por meios informáticos. O sigilo das comunicações é considerado pela Constituição[495] brasileira como um direito fundamental, conforme previsto no art. 5º, inciso XII.

Contudo, é necessário ressaltar que o direito ao sigilo, como todo direito fundamental, não é absoluto, conforme consta na Lei 9296/96[496], que versa sobre interceptação telefônica ou informática. Silva [497] explica que a interceptação se configura quando um terceiro, desconhecido pelas pessoas que estão trocando informações, consegue ter acesso à comunicação, não sendo necessário que ocorra a gravação desta. A mencionada lei trata-se de uma norma de exepcionalidade, só podendo ser aplicada nas situações previstas em seu art. 2º: quando houver indícios razoáveis da autoria ou participação em infração penal; nos casos em que a prova puder ser feita por outros meios disponíveis; quando o fato que está sendo investigado constituir infração penal punida com pena máxima de detenção.

Acerca do crime de violação de correspondência, previsto no art. 151 do Código Penal, entende-se que a norma deve abranger não apenas a correspondência física, mas também as mensagens trocadas por meios informáticos, conforme os ensinamentos de Silva[498]. Essa analogia se deve ao fato de que essas mensagens também são consideradas modalidades comunicação escrita, ainda que em meio cibernético.

Cabe ressaltar ainda que o Brasil é signatário da Convenção Americana de Direitos Humanos, também conhecida como Pacto de São José da Costa Rica, tendo o tratado entrado em vigor no território nacional em 25 de setembro de 1992[499]. Com a promulgação da Emenda Constitucional 45/2004 [500] , tratados que versam sobre direitos humanos vigoram imediatamente e são equiparados às normas constitucionais, desde que aprovados em dois turnos, por pelo menos três quintos dos votos na Câmara dos Deputados e no Senado Federal.

---

[495] BRASIL. **Constituição da República Federativa do Brasil**. Brasília, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 21 set. 2019.

[496] *Idem*. **Lei nº 9.296 de julho de 1996**. Regulamenta o inciso XII, parte final do artigo 5º da Constituição Federal. Brasília, DF, 24 jul. 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm. Acesso em: 21 set. 2019.

[497] SILVA, César Dario Mariano da. *Op. cit*., p. 118.

[498] *Ibidem*, p. 119

[499] BRASIL. **Decreto nº 678**, de 6 de novembro de 1992. Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 06 de novembro de 1992. Brasília, DF, 25 set. 1992. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/D3468.htm. Acesso em: 17 mar. 2020.

[500] *Idem*. **Emenda constitucional nº 45**, de 30 de dezembro de 2004. Altera dispositivos dos arts. 5º, 36, 52, 92, 93, 95, 98, 99, 102, 103, 104, 105, 107, 109, 111, 112, 114, 115, 125, 126, 127, 128, 129, 134 e 168 da Constituição Federal, e acrescenta os arts. 103-A, 103B, 111-A e 130-A, e dá outras providências. Brasília, DF, 30 dez. 2004. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc45.htm. Acesso em: 17 mar. 2020.

Dessa maneira, as disposições do Pacto de São José da Costa Rica apresentam status de normas constitucionais, de modo que o Brasil está vinculado ao cumprimento das mesmas. Para os fins desse trabalho, destaca-se novamente o art. 11 da Convenção Americana de Direitos Humanos:

> Artigo 11 - Proteção da Honra e da Dignidade
> 1. Toda pessoa tem direito ao respeito de sua honra e ao reconhecimento de sua dignidade.
> 2. Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação.
> 3. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas.

Uma das condenações sofridas pelo Brasil na CIDH ocorreu por violação a esse artigo. Em maio de 1999, um oficial da Polícia Militar do Paraná, denominado Waldir Copetti, solicitou a uma juíza na comarca de Loanda, no mesmo estado brasileiro, autorização para colocar escutas nas linhas telefônicas de cooperativas de trabalhadores vinculados ao Movimento dos Sem Terra (MST)[501]. A magistrada concedeu a autorização prontamente para que a escuta fosse instalada, porém não realizou o ato em conformidade com a legislação brasileira. Ela não notificou o Ministério Público e desconsiderou o fato de que a Polícia Militar não é competente para realizar investigações criminais contra civis.

As linhas telefônicas foram interceptadas durante 49 dias, entre abril e junho de 1999, sendo seus titulares os integrantes de organizações ligadas ao MST denominados Arley José Escher, Dalton Luciano de Vargas, Delfino José Becker, Pedro Alves Cabral, Celso Aghinoni e Eduardo Aghinoni[502]. Apesar de o Brasil ter sido notificado e tendo recebido um prazo de dois meses, prorrogado por três vezes, não atendeu às recomendações da Comissão Interamericana de Direitos Humanos.

O caso foi submetido à CIDH pela Comissão Interamericana de Direitos Humanos, que solicitou que o Brasil fosse condenado pela violação do art. 11 e de outros, em dezembro de 2007[503]. A CIDH divulgou a sentença em julho de 2009, condenando o Brasil pelo uso ilegal de interceptações telefônicas, bem como sua divulgação ilegal e impunidade dos responsáveis.

---

[501] CORTE INTERAMERICANA DE DIREITOS HUMANOS. **Caso Escher e Outros vs. Brasil**. Washington, 06 de julho de 2009. Disponível em: http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf. Acesso em: 17 mar. 2020.

[502] *Ibidem*. Disponível em: http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf. Acesso em: 17 mar. 2020

[503] *Ibidem*. Disponível em: http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf. Acesso em: 17 mar. 2020

No ano seguinte, cada um dos indivíduos que tiveram escutas colocadas em suas linhas telefônicas recebeu vinte e dois mil dólares a título de indenização[504].

Sobre a legislação mais recente sobre proteção à privacidade e à segurança informática, o ordenamento jurídico brasileiro possui a Lei nº 12.737/12[505], a retromencionada Lei Carolina Dieckmann. A pena para o crime de invasão de dispositivo informático é de três meses a um ano de detenção, de modo que é pouco provável que uma pessoa que cometa esse crime seja encarcerada. Pode ainda ser aumentada de um terço até a metade se o sujeito passivo do crime for: presidente da República; governador; prefeito; presidente do Supremo Tribunal Federal; Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

A eficácia da lei tem sido criticada especialmente após a Operação *Spoofing*, pois o cometimento desse crime contra juízes e promotores não acarreta aumento de pena. Vários advogados, juízes e membros do Ministério Público defenderam alterações no texto da Lei Carolina Dieckmann, inclusive a Associação de Juízes Federais do Paraná (APAJUFE) se manifestou favoravelmente nesse sentido para que seja proporcionada uma maior proteção aos magistrados[506]. Já houve uma condenação pelo crime previsto na Lei nº 12.737/12 no ano de 2017, quando um homem invadiu o celular do então governador do Distrito Federal, Rodrigo Rollemberg, tendo uma pena de oito meses de detenção, que foi substituída por prestação de serviço à comunidade[507].

Outra norma que alterou o Código Penal Brasileiro foi a Lei nº 13.772/2018[508], que acrescentou o art. 216-B, tipificando a conduta de divulgação não autorizada de conteúdo de

---

[504] BRASIL. **Decreto nº 7.158**, de 20 de abril de 2010. Autoriza a Secretaria de Direitos Humanos da Presidência da República a dar cumprimento a sentença exarada pela Corte Interamericana de Direitos Humanos. Brasília, DF, 20 abr. de 2010. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2010/decreto/D7158.htm. Acesso em: 17 mar. 2020.

[505] *Idem*. **Lei nº 12.737**, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.. Brasília, DF, 30 nov. de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 17 mar. 2020.

[506] LEI brasileira ainda é insuficiente para punir *hackers*. **Jornal O Sul**, 07 jul. 2019. Disponível em: https://www.osul.com.br/a-lei-brasileira-ainda-e-insuficiente-para-punir-*hackers*/. Acesso em: 17 mar. 2020.

[507] HOMEM que clonou celular de Rollemberg irá prestar serviços à comunidade. **Jornal de Brasília**, 24 jan. 2017. Disponível em: https://jornaldebrasilia.com.br/cidades/homem-que-clonou-celular-de-rollemberg-ira-prestar-servicos-a-comunidade/. Acesso em: 17 mar. 2020.

[508] BRASIL. **Lei nº 13.772**, de 19 de dezembro de 2018. Altera a Lei nº 11.340, de 7 de agosto de 2006 (Lei Maria da Penha), e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para reconhecer que a violação da intimidade da mulher configura violência doméstica e familiar e para criminalizar o registro não

intimidade sexual. Por meio dessa previsão normativa, o legislador brasileiro reconheceu que a ofensa à intimidade da mulher configura violência doméstica. A Lei nº 13.772/2018 prevê a pena detenção de seis meses a um ano, e multa para quem produzir, fotografar, filmar ou registrar, por qualquer meio, conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado sem autorização dos participantes. Aplica-se a mesma pena em casos de elaboração de montagem em fotografia, vídeo, áudio ou qualquer outro registro com o objetivo de incluir pessoa em cena de nudez ou ato sexual ou libidinoso de caráter íntimo. Trata-se de uma tentativa de diminuir os de divulgação não consentida de material íntimo.

Dentre a legislação mais recente sobre a salvaguarda à privacidade que não versa sobre matéria penal, é possível mencionar o Marco Civil da Internet, que estabeleceu os princípios a serem observados no uso da rede no Brasil. Um deles, previsto no art. 3º III, é justamente a proteção à intimidade. Além dessa lei há outro diploma normativo sobre o assunto previsto para entrar em vigor em agosto de 2019, a Lei nº 13.709/2018[509], conhecida como Lei Geral de Proteção de Dados (LGPD). Essa legislação dispõe sobre normas a serem observadas no processamento de informações pessoais, prevendo em seu art. 2º, I, o respeito à privacidade.

Como o problema metodológico desse trabalho possui como foco a legislação penal brasileira sobre o assunto, mais especificamente a Lei nº 12.737/12, na seção seguinte será examinado se a utilização da técnica hacker para invasão de um dispositivo informático pode ser considerada um crime conforme o art. 154-A ou outro artigo do código penal.

6 ANÁLISE DO *SPOOFING* CONFORME A LEGISLAÇÃO PENAL BRASILEIRA

Inicialmente, faz-se necessário ressaltar que o significado do termo "*spoofing*" pode ser utilizado para designar diversas práticas fraudulentas, para obter informações sigilosas de funcionários de empresas[510], por exemplo, ou manipulação de ativos na Bolsa de Valores[511]. Assim, nesse trabalho o uso da técnica estará restrito ao acesso desautorizado a ferramentas de

autorizado de conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado. Brasília, DF, 19 dez. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13772.htm. Acesso em: 17 mar 2020.

[509] BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Brasília, DF, 19 dez. 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 14 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 18 mar. 2020.

[510] BELVIC, Ivan. O que é spoofing e como posso me proteger dele?. **Avast**, 25 de jun. 2020. Disponível em: https://emprestimosim.com.br/blog/o-que-e-spoofing/. Acesso em: 18 out. de 2020.

[511] VOGLINO, Eduardo. O Que é Spoofing na Bolsa de Valores, a Nova Fraude Financeira. **The Capital Adivisor**, 26 ago. 2020. Disponível em: https://comoinvestir.thecap.com.br/o-que-e-spoofing-bolsa-de-valores/. Acesso em: 18 out. de 2020.

trocas de mensagens. Antes de verificar se a utilização do método denominado *spoofing* poderia encaixar-se em algum dos tipos penais existentes na legislação do Brasil, faz-se necessário abordar o conteúdo de um princípio que é considerado o pilar de diversos ordenamentos jurídicos do mundo ocidental.

A legislação penal brasileira é pautada pelo princípio da legalidade, assimilado pelo Estado moderno em decorrência da propagação da ideologia iluminista, de forma que o ordenamento pátrio se trata de um modelo jurídico liberal e garantidor. O referido princípio também é chamado de princípio da reserva legal pela maioria da doutrina. Contudo, existe uma corrente minoritária que considera o princípio da legalidade como gênero e o princípio da legalidade seria uma de suas espécies[512]. O princípio da legalidade tem por finalidade restringir o poder punitivo estatal, conforme será explanado a seguir.

Trata-se de uma consequência do reconhecimento da dignidade da pessoa humana, valor fundamental do Estado Democrático de Direito, cujos desdobramentos devem ser inclusos no âmbito do Direito Penal. Dessa forma, a integração de valores jurídicos liberais é a maneira mais favorável de evitar a possibilidade de o Estado se imiscuir, coercitivamente, na esfera de liberdade do indivíduo[513].

O princípio em questão é o reflexo da máxima do Positivismo dos séculos XVIII e XIX de que o ordenamento jurídico é completo e, sendo assim, não é permitida a existência de lacunas quanto à criminalização, ou seja, à configuração de tipos penais, e no que tange à tipicidade, a definição das condutas que identificam um comportamento considerado como criminoso. Ainda que estivessem presentes no ordenamento as chamadas "leis penais em branco", o conteúdo da mesma será fornecido pelo próprio sistema ou não haverá crime. Em linhas gerais, se o acontecimento corresponder à situação prevista em lei, configura-se um crime e cabe sanção, caso contrário não se pode considerar o sucedido como um fato criminoso[514].

---

[512] FREITAS JUNIOR, Dorival. Princípio Da Legalidade (Taxatividade da Lei) Como Garantia Da Dignidade Humana. **Centro Universitário Salesiano de São Paulo**, 2016, p. 17. Disponível em: http://unisal.br/hotsite/mostraderesponsabilidadesocial/wp-content/uploads/sites/11/2016/08/Artigo-Dorival-de-Freitas-Junior-T%C3%ADtulo-Princ%C3%ADpio-da-Legalidade-como-garantia_da_dignidade_humana.pdf. Acesso em: 19 out. de 2020.

[513]MINAHIM, Maria Auxiliadora de Almeida. Legitimação do Direito Penal por Princípios Reconhecidos e Inseridos nas Constituições de Estados Democráticos de Direito. **Revista da Faculdade Mineira de Direito**. Belo Horizonte, 2017, v. 20, n. 40, p. 72.

[514] LARAIA, Ricardo Regis. **A Dupla Face do Princípio da Legalidade**. Tese (Doutorado em Direito).

A primeira menção ao postulado "*nulla poena sine lege*" em uma obra escrita ocorreu no final do século XVIII. Paul Johann Anselm Ritter von Feuerbach, jurista alemão, formulou tal princípio latino em sua obra Tratado de Direito Penal, repetindo a mesma máxima em todas as edições dessa obra. Isso contribuiu, ao lado de outros fatos determinantes, para que os operadores do direito assimilassem o princípio da legalidade, que seria uma restrição aos poderes dos governantes[515].

Constata-se que tal premissa foi uma contribuição aportada pelo Iluminismo ao Direito Penal[516]. Um dos primeiros filósofos a tratar da noção de Estado de Direito foi o prussiano Immanuel Kant. Em sua obra "Fundamentação da Metafísica dos Costumes", o autor defende que as bases do Direito Penal são consequências do próprio Estado de Direito. Para Kant, o direito de punir contido na lei penal é o direito do magistrado, conferido pelo Estado de Direito, de causar algum prejuízo a pessoa que cometeu um crime[517].

O ideário iluminista pode ser compreendido como uma insurgência contra o absolutismo monárquico. A figura do monarca no antigo regime sintetiza-se na máxima "*L´Etat c´est moi*", atribuída ao rei Luís XVI. Em outras palavras, as ações estatais estavam subordinadas ao arbítrio do governante, que não apresentava quaisquer relações de subordinação às leis vigentes[518].

O sistema penal vigente até meados do século XVIII, antes da disseminação das retromencionadas ideias, possuía penas caracterizadas por sua crueldade, tendo o princípio da legalidade surgido para confrontar as práticas desumanas comuns desse sistema. O desenvolvimento do princípio da reserva legal tornou-se, assim, um recurso para estabelecer o alcance do poder de punir do Estado. A legalidade penal, em concordância com os demais dogmas defendidos pelo pensamento iluminista, se consolidou como uma segurança para os

---

Pontifícia Universidade Católica de São Paulo. São Paulo, 2008, p. 113.

[515] HRUSCHKA, Joachim. Kant, Feuerbach y los Fundamentos del Derecho Penal. In: MONTIEL, Juan Pablo (editor). **La crisis del principio de legalidade em el nuevo Derecho penal: ¿ decadência o evolución?**. Madrid: Marcial Pons, 2012, p. 88

[516] *Ibidem*, p. 87.

[517] KANT, Immanuel. **Metaphysical Elements of Justice: Part I of the Metaphysics of Morals**. Tradução de John Ladd. Cambridge: Hackett Publishing Company, 2 ed., 1999, p. 137.

[518] ARAÚJO, Fábio Roque. **O princípio da proporcionalidade referido ao legislador penal**. Salvador: Faculdade Baiana de Direito, 2011, p. 47.

indivíduos, viabilizando que a dignidade da pessoa humana, bem como a liberdade, fossem consagradas como valores do Estado democrático de Direito[519].

A limitação do poder do monarca pelo referido princípio estaria, assim, vinculada, estreitamente à demarcação do poder punitivo do Estado, agora restrito por princípios contidos na legislação, tais como o princípio da reserva legal e da proporcionalidade, por exemplo[520]. Em suma, o Direito Penal foi transformado em uma ferramenta para alcançar uma conjuntura de estabilidade entre o conceito de regulação, para garantir a salvaguarda de determinados bens jurídicos, e o entendimento de que o ser humano é detentor de alguns direitos. Esse pensamento foi efetivamente concretizado a partir da segunda metade do século XIX, à época do Estado intervencionista europeu[521].

A primeira Constituição brasileira, promulgada em 1824, sofreu alguma influência das ideias iluministas, como é possível perceber no inciso I do art. 179, de acordo com o qual nenhum cidadão estaria obrigado a fazer ou deixar de fazer algo, senão em virtude de lei[522]. A ingerência do pensamento ilustrado, consequentemente, também se fez presente na legislação penal, tendo o Código Criminal de 1830 previsto em seu primeiro artigo que não haveria crime ou delito, palavras sinônimas no referido texto normativo, sem uma lei anterior que o qualificasse[523].

O princípio da legalidade, atualmente, está previsto no inciso XXXIX do art. 5º da Constituição Federal [524] e no art. 1º do Código Penal brasileiro. Ademais, o Brasil é considerado um país engajado no que tange a tratados que versam sobre Direitos Humanos, sendo um dos Estados signatários do Pacto de San José da Costa Rica[525], o que significa que se comprometeu a orientar sua política em conformidade com as disposições do referido tratado.

---

[519] OLIVEIRA, Bruno Queiroz; CORREIO, Nestor Eduardo Santiago. A Crise da Legalidade Penal e a Função do Superior Tribunal de Justiça na Interpretação dos Tipos Penais. **Revista Eletrônica Direito e Sociedade**. Canoas, 2018, v. 6, n. 2, p. 42.
[520] ARAÚJO, Fábio Roque. *Op. cit.*, p. 48
[521] OLIVEIRA, Bruno Queiroz; CORREIO, Nestor Eduardo Santiago. *Op. cit*., p. 46.
[522] BRASIL. **Constituição Política do Império do Brazil**, Rio de Janeiro, 1824. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao24.htm. Acesso em: 16 abr. 2020.
[523] *Idem*. Lei de 16 de dezembro de 1830. Manda executar o Código Criminal. Rio de Janeiro, 1830.
[524] *Idem*. **Constituição da República Federativa do Brasil**. Brasília, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 20 set. 2019.
[525] COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS. **Convenção americana sobre direitos humanos**. San José, 1969. Disponível em: https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm. Acesso em: 20 set. 2019.

Dessa forma, há que se considerar o art. 9º do Pacto que se refere ao princípio da legalidade e da retroatividade. Conforme as disposições do tratado:

> **Ninguém poderá ser condenado por atos ou omissões que, no momento em que foram cometidos, não constituam delito, de acordo com o direito aplicável**. Tampouco poder-se-á impor pena mais grave do que a aplicável no momento da ocorrência do delito. Se, depois de perpetrado o delito, a lei estipular a imposição de pena mais leve, o delinquente deverá dela beneficiar-se. (Grifos nossos)

Ademais, cabe mencionar a construção teórica de Ferrajoli[526] acerca dos dez axiomas do garantismo penal:

> *A1) Nulla poena sine crimine* (Não há pena sem crime)
> *A2) Nullum crimen sine lege* (Não há crime sem lei)
> *A3) Nulla lex (poenalis) sine necessitate* (Não há lei penal sem necessidade)
> *A4) Nulla necessitas sine injusria* (Não há necessidade sem ofensa a bem jurídico)
> *A5) Nulla injuria sine actione* (Não há ofensa ao bem jurídico sem ação)
> *A6) Nulla actio sine culpa* (Não há ação sem culpa)
> *A7) Nulla culpa sine judicio* (Não há culpa sem processo)
> *A8) Nulla judicium sine accustone* (Não há processo sem acusação)
> *A9) Nulla accusatio sine probatione* (Não há acusação sem prova)
> *A10) Nulla probatio sine defensione* (Não há prova sem defesa)

Tais princípios são considerados a base do estado democrático de direito, conforme leciona Ferrajoli. De acordo com o autor italiano, o princípio da legalidade, previsto no primeiro axioma, demanda duas condições: o caráter formal ou legal do critério que define o comportamento desviante e a segunda é o caráter empírico ou fático das hipóteses de desvio estabelecidas em lei. Nos termos da primeira condição, o comportamento desviante não é definido conforme as características intrínsecas ou ontológicas percebidas na situação, mas sim pela indicação formal prevista em lei. Além disso, conforme a segunda condição, a definição de desvio não deve ser elaborada referindo-se a elementos subjetivos de status ou de autor, mas somente com referência a figuras de comportamento empíricas e objetivas[527].

Os mencionados axiomas servem como diretrizes para o Estado, de modo que a primazia da liberdade individual seja, obrigatoriamente, observada. Não há como compelir um Estado a adotar essa teoria, mas percebe-se que, no Brasil, os dogmas do garantismo são assimilados pelo ordenamento jurídico, posto que o princípio da legalidade apresenta status constitucional e está previsto expressamente no código penal[528].

---

[526] FERRAJOLI, Luigi. **Derecho y razón: Teoría del garantismo penal**. Madrid: Editorial Trotta, 1997, p. 93.
[527] *Ibidem*, p. 93-94.
[528] NOVELLI, Rodrigo Fernandes. A teoria do garantismo penal e o princípio da legalidade. **Revista Jurídica UNIGRAN**. Dourados, jan../jun. 2014, v. 16, n. 31, p. 128.

Sobre o vínculo do princípio da legalidade à noção de Estado democrático de direito, uma vez que se relaciona com a ideia de segurança jurídica, segundo Mir Puig, possibilita que todos os cidadãos possam saber quais ações podem realizar sem uma punição. Em outras palavras, trata-se de uma garantia política para o cidadão de que o Estado não poderá submetê-lo a penas que não são aceitas pelo povo. Apenas o povo de um Estado, por meio de seus representantes no Poder Legislativo, pode determinar quais condutas serão consideradas criminosas e suas respectivas penas[529].

Faz-se necessário também destacar o princípio da taxatividade, considerado um desdobramento do princípio da legalidade ou da determinação taxativa, de acordo com o qual é vedada a criação de tipos penais contendo expressões imprecisas, tendo como máxima a expressão latina "*nullum crimen, nulla poena sine lege certa*"[530].

No que tange à compreensão do texto normativo, o princípio da taxatividade refere-se ao seu destinatário também, com o intuito de fazê-lo entender de maneira que não reste dúvidas sobre seu conteúdo, para que a pena desempenhe sua utilidade intimidativa e com o intuito de salvaguardar o indivíduo do poder punitivo do Estado, representado pelo poder Judiciário[531]. Entende-se que um regime de proteção aos direitos de liberdade não pode ser ameaçado por tipos penais cujo preenchimento fique a critério do magistrado.

Dessa forma, o também chamado princípio da determinação vincula o legislador para que ele descreva o fato punível da forma mais exata possível, ou seja, a norma deve ser elaborada de maneira bastante clara na formulação do conteúdo do tipo penal e na previsão da sanção, para que haja garantia de segurança jurídica para os indivíduos[532].

Com essas breves análises sobre os princípios da legalidade e da taxatividade e referências a algumas das normas previstas no ordenamento jurídico brasileiro, questiona-se a possibilidade de o método de *spoofing*, na hipótese de sua utilização como meio para acessar um dispositivo, pode ser considerado um crime informático de acordo com a Lei nº 12.737/12.

---

[529] MIR PUIG, Santiago. **Derechos Humanos y Limites del Derecho Penal**. p. 466-467.
[530] SILVA, Louise Trigo da. Legalidade e taxatividade: a necessidade de definições e os tipos abertos. **Revista Eletrônica Direito e Política do Programa de Pós-Graduação Stricto Sensu em Ciência Jurídica da UNIVALI**, Itajaí, v.7, n.2, 2012, p. 1032.
[531] MINAHIM, Maria Auxiliadora de Almeida. *Op. cit*., p. 77.
[532] PRADO, Luiz Regis. **Curso de Direito Penal Brasileiro: parte geral e parte especial**. Rio de Janeiro: Editora Forense, 17a. ed. 2019, p. 158

O *spoofing*, termo que tem origem no verbo da língua inglesa "*to spoof*" (enganar, em português), é uma técnica que consiste em ludibriar uma pessoa ou burlar uma rede para que o indivíduo tenha acesso a uma conta de e-mail ou de um aplicativo alheia[533]. Dessa forma, o hacker pode enviar mensagens ou efetuar ligações, em casos de aplicativos que apresentem essa serventia, utilizando a conta em questão.

Ademais, esse método permite que hackers se apropriem do IP (sigla de *Internet Protocol*)[534], utilizado para identificar dispositivos e conexões a partir de uma sequência numérica, que funciona como o número de CPF de um indivíduo[535], e do DNS (sigla de *Domanin Name System*, sistemas de nomes de domínios), os responsáveis por identificar e traduzir para números IP os endereços dos sites buscados nos navegadores. Ao tomar posse do IP ou do DNS, os hackers podem enganar os usuários para que acessem sites falsos ou enviem mensagens por aplicativos[536].

O *spoofing*, ainda que seja uma técnica que não requer conhecimentos aprofundados na área da informática, se vale das falhas existentes nos sistemas das operadoras, prejudicando-as assim como os usuários, conforme elucidou o estrategista em segurança informática André Carraretto em uma entrevista para o site Canaltech[537]. Sendo apenas um método que consiste em ludibriar o usuário ou fraudar o sistema, o *spoofing* não é passível de eliminação por meio de programas *anti-malware*, também conhecidos como antivírus. Para proteger seus dispositivos é necessário, então, que as pessoas busquem algum conhecimento sobre técnicas de segurança informática.

No caso que deu ensejo à Operação *Spoofing*, realizada pela Polícia Federal, os hackers conseguiram invadir os celulares de autoridades ligadas à Operação Lava-Jato por meio de uma fragilidade técnica do sistema de caixa postal. O aplicativo em questão era o Telegram, cujo procedimento de autenticação para um novo acesso possui duas etapas. Inicialmente, um código de cinco dígitos é enviado pelo próprio Telegram, por meio de uma mensagem no

---

[533] RIBEIRO, Felipe. O que é spoofing? Conheça a técnica hacker utilizada contra Sérgio Moro. **Canaltech**, 26 jul. 2019. Disponível em: https://canaltech.com.br/hacker/covid-19-como-proteger-golpes-celular-utilizam-malwares-161991/. Acesso em: 23 mar. 2020.

[534] *Ibidem*. Disponível em: https://canaltech.com.br/hacker/covid-19-como-proteger-golpes-celular-utilizam-malwares-161991/. Acesso em: 23 mar. 2020.

[535] SALUTES, Bruno. O que é IP? **Canaltech**, 21 out. 2019. Disponível em: https://canaltech.com.br/software/o-que-e-ip/. Acesso em 23 mar. 2020.

[536] CIPOLI, Pedro. O que é DNS? **Canaltech**. Disponível em: https://canaltech.com.br/internet/o-que-e-dns/. Acesso em: 23 mar. 2020.

[537] RIBEIRO, Felipe. *Op. cit*. Disponível em: https://canaltech.com.br/hacker/covid-19-como-proteger-golpes-celular-utilizam-malwares-161991/. Acesso em: 23 mar. 2020.

aplicativo. Após essa etapa, há duas formas de solicitação do envio desse código para confirmar o acesso: por SMS ou por ligação[538].

Os hackers podem aproveitar essa última opção para colocar em prática o *spoofing*. Primeiramente, eles ligam diversas vezes para o número de celular do usuário, para que ele fique ocupado e a chamada não atendida do Telegram seja registrada na caixa postal. O serviço utilizado pelos hackers para fazer a ligação pela Internet, mascarando o número que está ligando, chama-se *VOIP* (*voice over IP*), aparentando, por vezes que a pessoa está recebendo uma ligação de seu próprio número[539].

Quando a vítima não atende à ligação do Telegram, o aplicativo deixa uma mensagem na caixa postal. Ocorre que uma das formas de acessar a caixa postal, conferindo ao sistema uma falha que torna o *spoofing* possível, é ligar para o próprio número. O hacker efetua uma chamada que tem sua origem falsificada, como se fosse o próprio número do usuário. Assim, ele consegue acessar a caixa de mensagens, escutar a mensagem de autenticação do Telegram e conectar-se ao aplicativo. Foi essa a estratégia utilizada pelos responsáveis pelos acessos não-autorizados às contas de Telegram das pessoas ligadas à Operação Lava-Jato[540].

Em julho de 2019, uma deputada chegou a afirmar que o Palácio do Planalto poderia invocar a Lei de Segurança Nacional para denunciar as pessoas acusadas de invadir o celular do então Ministro da Justiça e Segurança Pública e outras autoridades, pois os atos praticados por esses indivíduos poderiam ser considerados terroristas[541]. Esse entendimento, contudo, não é o mais adequado, sendo necessário recorrer à Lei nº 13.260, de 16 de março de 2016, que traz a definição de terrorismo.

Também chamada de Lei Antiterrorismo, embora a referida lei trate em seu art. 2º, § 1º, IV, do ciberterrorismo, a conduta tipificada é sabotar o funcionamento ou apoderar-se, com

---

[538] ROHR, Altieres; LAVADO, Thiago. 'Spoofing': como foi a invasão do celular de Sérgio Moro, segundo a decisão judicial que mandou prender 4 suspeitos. **G1**, 24 jul. 2019. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2019/07/24/spoofing-como-foi-a-invasao-do-celular-de-sergio-moro-segundo-a-decisao-judicial-que-mandou-prender-4-suspeitos.ghtml. Acesso em: 23 mar. 2020.

[539] *Ibidem*. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2019/07/24/spoofing-como-foi-a-invasao-do-celular-de-sergio-moro-segundo-a-decisao-judicial-que-mandou-prender-4-suspeitos.ghtml. Acesso em: 23 mar. 2020.

[540] *Ibidem*. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2019/07/24/spoofing-como-foi-a-invasao-do-celular-de-sergio-moro-segundo-a-decisao-judicial-que-mandou-prender-4-suspeitos.ghtml. Acesso em: 23 mar. 2020.

[541] FORTES, Carolina. Lei de Segurança Nacional não poderia ser aplicada para hackers de Moro, diz especialista. **Jovem Pan**, 27 jul. de 2019. Disponível em: https://jovempan.com.br/noticias/brasil/lei-de-seguranca-nacional-nao-poderia-ser-aplicada-para-hackers-de-moro-diz-especialista.html. Acesso em: 19 out. 2020.

violência, grave ameaça a pessoa ou utilizando mecanismos cibernéticos, do controle total ou parcial, mesmo que de maneira temporária, de meio de comunicação ou de transporte, de portos, aeroportos, estações ferroviárias ou rodoviárias, hospitais, casas de saúde, escolas, estádios esportivos, instalações públicas ou locais onde funcionem serviços públicos essenciais, instalações de geração ou transmissão de energia, instalações militares, instalações de exploração, refino e processamento de petróleo e gás e instituições bancárias e sua rede de atendimento. Em suma: a conduta praticada por esses indivíduos não se amoldaria a esse tipo penal.

Cabe ainda destacar que uma forma similar de invasão de contas de aplicativo tem se tornado bastante popular pelos delinquentes informáticos no Brasil: uma fraude que ficou conhecida como "golpe do WhatsApp"[542]. Muitas pessoas já foram vítimas ou sofreram tentativas desse golpe, uma vez que o de um aplicativo está presente em noventa e nove por cento dos smartphones brasileiros[543].

Nessa fraude, o usuário recebe um código de seis dígitos por WhatsApp e, em seguida, uma pessoa entra em contato pelo próprio aplicativo informando que a mensagem era destinada a outro número. A pessoa pede que a vítima compartilhe esse código com ela, conseguindo, assim, acesso à conta do aplicativo da vítima. Isso ocorre porque os golpistas tentam cadastrar o número do usuário em outro dispositivo, sendo essa verificação necessária. Com o compartilhamento do código, os hackers acessam a conta do WhatsApp da vítima e conversam com seus contatos, normalmente pedindo quantias emprestadas, se passando pelo titular da conta do aplicativo[544].

Conforme mencionado, o *spoofing* pode ser considerado uma espécie de ardil para ludibriar o titular de uma conta de e-mail ou de aplicativos de mensagens instantâneas para que outra pessoa consiga ter acesso a mesma. Contudo, não se trata de um método de interferência nas ferramentas de segurança do dispositivo informático, de forma que tal conduta não se amolda ao tipo penal descrito na Lei Carolina Dieckmann

---

[542] NOGUEIRA, Luiz. Novo golpe do WhatsApp invade contas com o código de verificação. **Olhar Digital**, 28 fev. 2020. Disponível em: https://olhardigital.com.br/fique_seguro/noticia/novo-golpe-do-whatsapp-invade-contas-com-o-codigo-de-verificacao/97388. Acesso em: 23 mar. 2020.

[543] GATTIS, Nina. WhatsApp está em 99% dos celulares no Brasil. **Olhar Digital**, 27 fev. 2020. Disponível em: https://olhardigital.com.br/noticia/whatsapp-esta-em-99-dos-celulares-no-brasil/97355. Acesso em: 23 mar. 2020.

[544] NOGUEIRA, Luiz. *Op. cit*. Disponível em: https://olhardigital.com.br/fique_seguro/noticia/novo-golpe-do-whatsapp-invade-contas-com-o-codigo-de-verificacao/97388. Acesso em: 23 mar. 2020.

Segundo o art. 154-A, acrescido ao Código Penal brasileiro pela suprareferida lei, é considerada criminosa a seguinte ação:

> **Invasão de dispositivo informático**
> Art. 154-A. Invadir **dispositivo informático** alheio, conectado ou não à rede de computadores, **mediante violação indevida de mecanismo de segurança** e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. (Grifos nossos)

Na área de sistemas da informação, uma invasão é descrita como um mecanismo utilizado para identificar falhas ou informações em redes ou dispositivos eletrônicos. Para aprimorar a segurança de redes e sistemas, são realizados testes nos quais busca-se explorar brechas dos mesmos, identificando seus pontos mais vulneráveis[545]. Talvez a conduta de *spoofing* pudesse ser classificada como uma "invasão informática" de acordo com essa definição técnica, mas certamente não poderia ser interpretada como uma "invasão de dispositivo informático" nos moldes do artigo supracitado, conforme será explanado mais adiante.

Ressalte-se que a Lei nº 12737/2012 não apresenta um texto suficientemente preciso. Conforme mencionado anteriormente, trata-se de uma lei aprovada de maneira bastante célere. Ela foi sancionada em dezembro de 2012, cinco meses após a situação envolvendo o acesso não autorizado ao computador da atriz Carolina Dieckmann para chantageá-la com a ameaça de divulgar fotos íntimas, tendo entrado em vigor em abril do ano seguinte[546]. Como o caso envolveu uma pessoa pública, a rapidez com a qual foi aprovado o Projeto de Lei 2793/2011[547] prejudicou a qualidade do texto normativo.

Antes do referido projeto de lei ser proposto, é necessário destacar que já havia outro que versava sobre crimes informáticos tramitando na Câmara dos Deputados desde 1999. O Projeto de Lei 84/1999[548] foi transformado na Lei nº 12735/2012, a chamada Lei Azeredo,

---

[545] SILVA, Taís Cristina da; LOZI, Diêgo Pereira; SOUZA, Gabriel Aguiar Tinti de; CANCELA, Lucas Borcard. Técnicas de Invasão: um estudo sobre as armas do mundo digital. **Anais do Encontro Virtual de Documentação em Software Livre e Congresso Internacional de Linguagem e Tecnologia Online**, 2019, v. 8, n. 1.

[546] LEI 'Carolina Dieckmann', que pune invasão de PCs, entra em vigor. **G1**, 01 de abril de 2013. Disponível em: http://g1.globo.com/tecnologia/noticia/2013/04/lei-carolina-dieckmann-que-pune-invasao-de-pcs-passa-valer-amanha.html. Acesso em: 24 mar. 2020.

[547] BRASIL. Câmara dos Deputados. **Projeto de Lei 2793/2011**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Brasília, DF, 29 de novembro de 2011. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=529011. Acesso em: 24 mar. 2020.

[548] *Idem*. Câmara dos Deputados. **Projeto de Lei 84/1999**. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal e a Lei nº 9.296, de 24 de julho de 1996, e dá outras providências. Brasília, DF, 24 de

sofreu a exclusão da maior parte de seu conteúdo original. Antes desse projeto, houve outro relacionado à criminalidade informática proposto em 1991, que foi abandonado na Câmara dos Deputados[549].

O texto da Lei Carolina Dieckmann não elucida termos como "dispositivo informático" ou "mecanismo de segurança", o que proporciona uma insegurança acerca do entendimento do tipo penal incluído por meio da norma. Para Sydow, partindo do pressuposto que a palavra "dispositivo" seria utilizada para designar uma peça ou máquinas em proporções menores[550], um dispositivo informático seria qualquer hardware para processar e armazenar dados[551]. A palavra "hardware" designa peças físicas no campo da tecnologia da informação, como processador, placa-mãe ou unidades de armazenamentos (HDs)[552]. Assim, ficariam excluídos serviços disponíveis apenas no ciberespaço, como e-mails ou contas de aplicativos.

Uma matéria disponibilizada pelo G1, portal de notícias do Grupo Globo, consultou alguns especialistas na área para esclarecer a aplicação da Lei de Crimes Cibernéticos. Para deles, Renato Opice Blum[553], só entravam no âmbito de proteção da referida lei máquinas que possuíssem alguma ferramenta de segurança, como um *firewall* ou uma barreira de hardware. Enquanto os *firewalls* [554]são aplicativos ou equipamentos que conferem e filtram o fluxo de dados, uma barreira de hardware[555] seria uma estrutura desenvolvida pela engenharia da computação com o objetivo de garantir a proteção de estruturas de dados compartilhados.

---

fevereiro de 1999. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=15028. Acesso em: 24 mar. 2020.

[549] ROHR, Altieres. Sem lei específica, Brasil discute cibercrimes há 20 anos, diz advogado. **G1**, 29 jun. 2011. Disponível em: http://g1.globo.com/tecnologia/noticia/2011/06/sem-lei-especifica-brasil-discute-cibercrimes-ha-20-anos-diz-advogado.html. Acesso em: 24 mar. 2020.

[550] DISPOSITIVO in **Dicionário Brasileiro da Língua Portuguesa Michaelis**. Disponível em: https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/dispositivo/. Acesso em: 18 out. 2020.

[551] SYDOW, Spencer Toth. **Curso de Direito Penal Informático – Parte Geral e Especial,** Salvador: Jus Podium, 2020, p. 441.

[552] GOGONI, Ronaldo. O que é um hardware? **Tecnoblog**. Disponível em: https://tecnoblog.net/311761/o-que-e-hardware/. Acesso em: 18 de out. de 2020.

[553] BLUM, Renato Opice. Depoimento para o Portal G1. Lei 'Carolina Dieckmann' só vale para PCs protegidos, diz advogado, **G1**, 04 dez. 2012. Disponível em http://g1.globo.com/tecnologia/noticia/2012/12/lei-carolina-dieckann-so-vale-para-pcs-protegidos-diz-advogado.html. Acesso em: 24 mar. 2020.

[554] MACHADO, Jonathan. O que é firewall? **Techmundo**, 21 jun 2018. Disponível em: https://www.tecmundo.com.br/firewall/182-o-que-e-firewall-.htm. Acesso em: 24 mar. 2020.

[555] ABELLÁN, José L.; ACACIO, Manuel E.; FERNÁNDEZ, Juan Esteban. Efficient Hardware Barrier Synchronization in Many-Core CMPs. **IEEE Transactions on Parallel and Distributed Systems**. Nova York, ago. 2012, v. 23, p. 1.

Para outro especialista no assunto, Victor Haikal[556], como o texto não define o que seria um "mecanismo de segurança", se a máquina tiver uma senha, já apresenta um recurso a ser violado. Ademais, Opice Blum[557] explicou que, de acordo com o texto da Lei de Crimes Informáticos, as invasões realizadas através de redes *Wi-Fi* abertas não se encaixam no tipo penal descrito no art. 154-A, uma vez que não há qualquer ferramenta de segurança informática nas referidas redes, sendo aconselhável, assim, a implementação de senhas nas mesmas.

Mecanismos de segurança podem ser compreendidos como todos aqueles que objetivam restringir o acesso de terceiros não autorizados a um sistema informático e assegurar a autenticidade do detentor legítimo do acesso. Exemplos dessas ferramentas como autenticação por meio de dois fatores, cartões de numeração, criptografia, esteganografia, impressão palmar, leitura de íris, senhas e tokens. Todos os mecanismos têm por finalidade diminuir a chance de acessos ilegítimos e garantir que o usuário legítimo conceda permissão para uso e modificação de um sistema, de acordo com Sydow[558].

Entretanto, um entendimento mais restrito sobre o conceito da expressão "mecanismos de segurança" também pode ser adotado. Segundo o site IBM Knowledge Center, pertencente à empresa de serviços informáticos IBM, tais mecanismos são ferramentas técnicas e métodos que empregados para instalar serviços de segurança. Eles podem operar por conta própria ou com outros para fornecer um determinado serviço específico. Os mecanismos de segurança mais comuns são: os certificados digital, atestados para garantir que um documento pertence a certa pessoa ou entidade; a criptografia, processo por meio do qual um texto legível é transformada em uma mensagem cifrada; trechos de mensagens, que são representações numéricas de tamanho fixo do conteúdo de mensagens; a Infraestrutura da Chave Pública[559]

---

[556] HAIKAL, Victor. Depoimento para o Portal G1. Lei 'Carolina Dieckmann' só vale para PCs protegidos, diz advogado, **G1**, 04 dez. 2012. Disponível em: http://g1.globo.com/tecnologia/noticia/2012/12/lei-carolina-dieckann-so-vale-para-pcs-protegidos-diz-advogado.html. Acesso em: 24 mar. 2020.

[557] BLUM, Renato Opice. *Op. cit*. Disponível em: http://g1.globo.com/tecnologia/noticia/2012/12/lei-carolina-dieckann-so-vale-para-pcs-protegidos-diz-advogado.html. Acesso em: 24 mar. 2020.

[558] SYDOW, Spencer Toth. *Op. cit.*, p. 443.

[559] A criptografia de chave pública ou criptografia de chaves assimétricas consiste no uso de utiliza duas chaves distintas, sendo uma pública, que pode ser livremente divulgada, e uma privada, que deve ser mantida em segredo por seu titular. No momento em que uma informação é codificada com uma das chaves, apenas a outra chave do par pode decodificá-la. A utilização de cada chave usar para codificar dependerá da proteção que se pretende, se confidencialidade ou autenticação, integridade e não-repúdio. Ademais, existe a criptografia de chave secreta ou única, também chamada de criptografia de chave simétrica, método que dispõe de uma mesma chave tanto para codificar como para decodificar informações, sendo usada principalmente para assegurar a confidencialidade dos dados. Situações em que a informação é codificada e decodificada por uma mesma pessoa não acarretam necessidade de compartilhamento da chave secreta. Contudo, quando estas operações envolvem

(tradução do termo *Public Key Infrastructure*), um sistema de recursos, políticas e serviços com a finalidade de viabilizar o uso de criptografia de tecla pública para autenticar as partes envolvidas em uma transação[560].

Constata-se, dessa forma, que a Lei Carolina Dieckmann não apresenta temos suficientemente precisos, o que dificulta a sua aplicação, e, especialmente, por conta de seu processo de elaboração e aprovação[561]. Sobre o último, como retromencionado, foi por demais célere e não houve muitas discussões acerca do texto da lei. Contudo, além desse fato, o processo de concepção da Lei sobre Crimes Informáticos, conforme ressaltado por Sydow, não contou com a busca das necessidades da população, tampouco foram consultados profissionais da área informática ou jurídica, especialmente a academia, que estuda com mais profundidade as questões do Direito Informático. Há também o empecilho da falta de capacitação dos membros da polícia, do Judiciário e do Ministério Público para lidar com os problemas existentes na sociedade da informação, assim, poder participar da construção da lei[562].

Admitindo que o Brasil adota o sistema da reserva legal, Jesus e Milagres[563] destacam que as leis sobre tecnologia da informação devem ser criadas por meio de uma técnica específica, pois, assim, o legislador evita que a norma inicie o seu período em vigor já ultrapassada.

Para elaborar leis eficazes e que prescindam de complementação no futuro, os autores defendem que seja utilizada a teoria TCC: técnica, comportamento e crime. A técnica seria qualquer método ou processo informático utilizado que caracterize um comportamento, podendo ser executada de forma manual ou por meio do uso de ferramentas. O comportamento, por sua vez, seria uma ação efetuada mediante uma técnica ou mais, praticada por um ou mais agentes em relação a redes, dispositivos ou sistemas informáticos.

---

indivíduos ou equipamentos diferentes, é preciso que a chave secreta seja previamente combinada por meio de um canal de comunicação seguro, com o intuito de não comprometer a confidencialidade da chave. CENTRO de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha De Segurança Para Internet - Criptografia**. Disponível em: https://cartilha.cert.br/criptografia/. Acesso em 18 out. 2020.

[560] CONCEITOS e Mecanismos de Segurança. **IBM Knowledge Center**. Disponível em: https://www.ibm.com/support/knowledgecenter/pt-br/SSFKSJ_8.0.0/com.ibm.mq.sec.doc/q009730_.htm. Acesso em: 18 out. 2020.

[561] SYDOW, Spencer Toth. Entrevista disponibilizada no portal DM.JOR.BR. Impunidade cibernética. **Diário da Manhã**, 17 ago. 2016. Disponível em: https://www.dm.jor.br/politica/2016/08/impunidade-cibernetica/. Acesso em: 24 mar. 2020.

[562] SYDOW, Spencer Toth. **Curso de Direito Penal Informático – Parte Geral e Especial,** Salvador: Jus Podium, 2020, p. 295.

[563] JESUS, Damásio de; MILAGRES, José Antonio. *Op. cit.*, p. 29.

Já o crime seria um ou diversos comportamentos cometidos com a utilização e uma ou mais técnicas que viole um bem jurídico protegido pelo Direito[564].

Tomando essa teoria como ponto de partida, chega-se à premissa de que não é viável criar leis sobre técnicas, pois qualquer tentativa nesse sentido tornaria a legislação antiquada rapidamente, uma vez que os métodos desenvolvidos pela informática estão em constante evolução. Assim, é preciso distinguir um comportamento, desempenhado por uma ou por várias técnicas informáticas, que seja reprovável o suficiente para ser considerado um crime. Os autores, então, entendem que, em matéria de Direito Penal Informático, é de suma importância examinar qual conduta pode ser considerada criminosa, ainda que ela possa ser realizada de várias maneiras[565].

A compreensão dos autores sobre a percepção equivocada dos legisladores brasileiros, que confundem técnica e conduta, juntamente com a percepção da falta suporte técnico na área de tecnologia da informação para apoiar o Poder Legislativo, faz eco com a perspectiva de Sydow[566], que também considera que os responsáveis pela criação das leis não buscam especialistas para auxiliá-los durante esse processo de construção legislativa.

O legislador brasileiro, ciente de que o modelo jurídico-penal do país tem como pilar fundamental o princípio da legalidade, não pode empregar termos por demais imprecisos no texto normativo. Trata-se de uma premissa dirigida ao legislador que contém uma proibição de elaborar normas penais indeterminadas, de forma que deve precisar expressamente as hipóteses de violação a um bem jurídico que são consideradas como crimes[567].

Ainda que no art. 4º da Lei de Introdução ao Código Civil[568] esteja prevista a possibilidade de o magistrado respaldar suas decisões nos costumes, princípios gerais do direito e analogias, tal disposição não pode ser aplicada ao Direito Penal, pois, se um fato não estiver previsto em lei como um ilícito punível, deve ser considerado uma conduta lícita, por conta do princípio da legalidade.

---

[564] *Ibidem*, p. 29-30.
[565] *Ibidem*, p. 30.
[566] SYDOW, Spencer Toth. *Op. cit*., p. 295.
[567] KUHLEN, Lothar. Sobre la Relación entre el Mandato de Certeza y la Prohibición de la Analogía. In: MONTIEL, Juan Pablo (editor). **La crisis del principio de legalidade em el nuevo Derecho penal: ¿ decadência o evolución?.** Madrid: Marcial Pons, 2012, p. 179.
[568] BRASIL. **Decreto-lei nº 4.657, de 4 de setembro de 1942**. Lei de Introdução às normas do Direito Brasileiro. Brasília, 04 set. 1942. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del4657.htm. Acesso em :18 abr. 2020.

Na análise do referido princípio, considerando o viés do seu conteúdo, é preciso atentar que a determinação da conduta ilícita em lei, por um lado significa "dispor sobre um assunto" e, por outro, "assumir uma prescrição de forma clara", conforme ressalta Kuhlen. Dessa forma, a lei deve prescrever a punibilidade de ações determinadas e, de acordo com o entendimento majoritário, impor o estabelecimento das consequências jurídicas de um fato punível[569].

É certo que o mesmo princípio também apresenta consequências para os intérpretes das leis, admitindo que o resultado da indagação é variável. De maneira abstrata, a resposta é positiva, pois considera-se que o intérprete não pode efetuar entendimentos extravagantes sobre o texto legal, tampouco deve valer-se de analogias. Por outro lado, é possível considerar que o princípio da legalidade não tem consequências para o intérprete, pois os parâmetros para definir o alcance do processo interpretativo nem sempre são exatos[570].

Em casos nos quais a lei se omite, o intérprete pode buscar a solução para a contenda no raciocínio analógico, ampliando, assim, o âmbito de aplicação da norma para abarcar situações similares[571]. Sabe-se que no âmbito do Direito Penal há duas espécies de analogia. A analogia *in malam partem* determina que em situações não contempladas pela legislação, porém similares, é viável a aplicação da pena, enquanto a analogia *in bonam partem* estipula que, na conjuntura retromencionada, não caberia uma sanção[572].

O uso desse método interpretativo em normas penais incriminadoras é restrito, uma vez que não admite a analogia *in malam partem*, sob o risco de violar o princípio da legalidade, previsto na Constituição Federal e no Código Penal brasileiro. Essa limitação do emprego da analogia se dá porque a finalidade da lei é prescrever tão somente as condutas que devem ser consideradas ilícitos penais[573].

Assim, constata-se que, no sistema penal brasileiro, é vedado o uso da analogia *in malam partem*, porém é possível que a analogia *in bonam partem* seja aplicada, uma vez que

---

[569] KUHLEN, Lothar. *Op. cit*., p. 156-157.
[570] GIMENO, Iñigo Ortiz de Urbina. ¿Leyes taxativas interpretadas libérrimente? Princípio de Legalidad e Interpretación del Derecho Penal. In: MONTIEL, Juan Pablo (editor). **La crisis del principio de legalidade em el nuevo Derecho penal: ¿ decadência o evolución?.** Madrid: Marcial Pons, 2012, p. 179.
[571] MARTINS, José Salgado. A Analogia e o Princípio de Individualização em Matéria Penal. **Conferência proferida na sessão de encerramento do Congresso Estadual do Ministério Público do Rio Grande do Sul**. Porto Alegre, junho de 1957. Disponível em: seer.ufrgs.br. Acesso em: 22 out. 2020.
[572] Ibidem. Disponível em: seer.ufrgs.br. Acesso em: 22 out. 2020.
[573] PRADO, Luiz Regis. *Op. cit.*, p. 208.

beneficia o réu. Nesse sentido, Martins[574] elucida que o impedimento da analogia se aplica apenas às normas penais, uma vez que não é possível ampliar seu campo de incidência. Entretanto, é preciso ressaltar que o emprego da analogia *in bonam partem* pressupõe que exista uma lacuna na lei, mas não pode haver um emprego dessa analogia quando estiver claro no texto da norma que a finalidade da norma era a de excetuar da regulação certos casos similares[575].

Tal posicionamento pode ser encontrado inclusive nas decisões de tribunais brasileiros[576]:

> Em Direito Penal, o princípio da reserva legal exige que os textos sejam interpretados sem ampliações ou equiparações por analogia, salvo quando *in bonam* parte. Ainda vige o aforismo *poenalia sunt restringenda*, ou seja, interpretam-se estritamente as disposições cominadoras de pena.

Ressalte-se que compromisso dos operadores do Direito Penal não é, ao menos de forma imediata, com o Estado de Direito e com a separação dos poderes, mas com a contenção do poder punitivo estatal, conforme destaca Gimeno[577]. Malgrado esse seja um propósito bastante nobre, que envolve, ainda que indiretamente, a proteção da dignidade humana, esse posicionamento pode causar prejuízos aos anseios sociais, objetos de atenção do legislador. Dessa forma, para que legisladores e operadores do Direito possam trabalhar em parceria para combater a criminalidade informática, se faz necessária uma elaboração mais cuidadosa de leis nesse sentido.

O *spoofing* é uma técnica que consiste em acessar um dispositivo informático por meio da usurpação da identidade do usuário legítimo, valendo-se de uma brecha no sistema de segurança[578]. Não há violação de qualquer ferramenta de salvaguarda do dispositivo. De acordo com informações disponibilizadas no *site* da *Malwarebytes*[579], o sucesso do uso do *spoofing* não se deve somente à técnica propriamente dita, que conta com falhas de segurança, mas aos métodos que os criminosos usam para enganar as pessoas[580]. Considerando que ainda

---

[574] *Ibidem, loc. cit.*
[575] TOLEDO, Francisco de Assis. **Princípios Básicos de Direito Penal**, 4a ed. São Paulo: Saraiva, 1991, p. 27.
[576] SÃO PAULO. Tribunal de Alçada Criminal de São Paulo. Ação Criminal. Relator Adauto Suannes. **Revista dos Tribunais 594/355**.
[577] GIMENO, Iñigo Ortiz de Urbina. *Op. cit*., p. 181-182.
[578] DIFFERENCE between Spoofing and Phishing. **GeeksforGeeks**, New Okhla Industrial Development Authority. Disponível em: https://www.geeksforgeeks.org/difference-between-spoofing-and-phishing/. Acesso em: 26 mar. 2020.
[579] Empresa estadunidense fornecedora de serviços de cibersegurança, tendo sido indicada a vários prêmios na área de segurança informática e vencido.
[580] SPOOFING. **Malwarebytes**, Santa Clara. Disponível em: https://www.malwarebytes.com/spoofing/. Acesso em: 26 mar. 2020.

não há uma cultura consolidada de educação informática no Brasil, a tarefa de enganar o proprietário de uma conta de e-mail ou de aplicativo não é muito complexa.

Como não há a possibilidade de instalar um antivírus para evitar o *spoofing*, mesmo porque não se trata de um software malicioso, mas de uma técnica para usurpar a identidade do titular de uma conta de e-mail/aplicativo ou de uma máquina, é preciso ter alguma cautela no ambiente cibernético para não se tornar uma vítima desse ardil. A *Forcepoint*[581] menciona algumas recomendações, como a de que os usuários de smartphones prestem atenção aos números que estão ligando ou mandando mensagens por aplicativos, pois podem se tratar de hackers tentando empregar esse método para acessar seu dispositivo. Já as empresas devem investir em meios para aperfeiçoar os seus mecanismos de segurança voltados para proteger os serviços por elas disponibilizados, pois, no caso que motivou a Operação *Spoofing*, se não houvesse uma vulnerabilidade técnica no sistema da caixa postal, os hackers não teriam como acessar os celulares das pessoas envolvidas na Operação Lava jato[582].

O uso de *spoofing* na retromencionada situação, como não se trata de uma violação a um mecanismo de segurança, não se amolda ao tipo penal do art. 154-A do Código Penal brasileiro. Existe, conforme elucidam Jesus e Milagre[583], um paradigma a ser superado, sendo necessário distinguir técnica, artefato e comportamento, de forma que o operador do Direito deve examinar cada técnica para verificar se ela se amolda ou não ao tipo penal.

O operador do Direito que atua com casos de crimes informáticos precisa ter noções técnicas dessa área, uma vez que há métodos empregados para cometer tais delitos que não preenchem os requisitos dispostos no tipo penal. Em suma: é necessário conhecer tais procedimentos para evitar injustiças. Enquanto os advogados podem empregar conhecimentos informáticos para realizarem defesas, as autoridades policiais e judiciárias devem atentar para não desempenharem sua atuação com base na premissa de que "não importa a técnica utilizada, o importante é a conduta" para evitar violações ao princípio da legalidade[584].

---

[581] Empresa estadunidense fornecedora de serviços de cibersegurança, referência na área por prestar serviços para grandes corporações como *Boeing*, *Toyota* e *Walmart*.

[582] ROHR, Altieres; LAVADO, Thiago. *Op. cit.* Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2019/07/24/spoofing-como-foi-a-invasao-do-celular-de-sergio-moro-segundo-a-decisao-judicial-que-mandou-prender-4-suspeitos.ghtml. Acesso em: 23 mar. 2020.

[583] JESUS, Damásio de; MILAGRE, José Antonio. *Op. cit*., p. 31

[584] *Ibidem*, p. 32.

Considerando que os termos empregados no texto legal são passíveis de mais de uma interpretação, a ciência jurídica considera viável que exista um determinado grau de imprecisão, de acordo com Bitencourt[585]. Quando o legislador utiliza muitas expressões que demandam complementação valorativa, ou seja, que não especificam qual é a conduta proibida no tipo penal, é provável que o princípio da reserva legal seja desrespeitado em algum momento da aplicação da norma. Por outro lado, o referido autor admite que os conceitos valorativos, também chamados de cláusulas gerais, possibilitam que a norma se adeque com mais acerto à conduta proibida. Bitencourt sugere que seja buscado um ponto de equilíbrio entre as duas situações mencionadas, para que os bens jurídicos sejam protegidos sem que haja violação ao princípio da legalidade[586].

No caso da Lei Carolina Dieckmann, o tipo penal incluído no Código Penal brasileiro apresenta vários elementos imprecisos. Um dos elementos necessários, nos termos do art. 154-A, é a existência de um "dispositivo informático", mas a lei não traz qualquer definição desse termo. Sydow[587], partindo da premissa que a palavra "dispositivo" é um sinônimo de "máquina", entende que qualquer hardware pode ser considerado um dispositivo informático nos termos da referida legislação. Dessa forma, não seriam protegidos serviços prestados de forma exclusivamente on-line, como as contas de e-mails e de aplicativos, softwares, que são bens imateriais, e tampouco aparelhos eletrônicos que não tenham como finalidade específica a utilização no ambiente informático e que não detenham dados sigilosos, como, por exemplo, um relógio como o Apple Watch[588]. Alguns dos aparelhos protegidos por essa lei seriam os smartphones, computadores e notebooks.

Dessa maneira, caso um hacker se valesse do *spoofing* para acessar uma conta de e-mail ou de aplicativo, talvez não fosse possível enquadrar essa conduta no tipo penal descrito no art. 154-A do Código Penal. Isso porque se tratam de serviços utilizados somente no ambiente cibernético, não havendo suporte de uma máquina. Essa é uma das questões que resultam da imprecisão dos elementos do tipo penal, como o termo "dispositivo informático".

Outro obstáculo para a aplicação do tipo descrito no art. 154-A é a falta de definição do termo "mecanismo de segurança" na norma penal. Para Sydow, os mecanismos de segurança seriam

---

[585] BITENCOURT, Cezar Roberto. **Tratado de Direito Penal,** 10ª. ed., São Paulo: Saraiva, 2006, p. 15.
[586] *Ibidem, loc. cit.*
[587] SYDOW, Spencer Toth. *Op. cit.*, p. 298.
[588] Trata-se de um relógio que pode se conectar ao smartphone, possibilitando ao usuário efetuar chamadas, receber mensagens e utilizar aplicativos. Essa nova geração de relógios é denominada *smartwatch*.

todos os que objetivam impedir o acesso de terceiros sem permissão a um sistema informático, garantindo assim a proteção do dispositivo e a autenticidade do titular legítimo de acesso. Seriam, assim, exemplos de mecanismos de segurança as senhas, *tokens* e cartões de numeração[589]. O *spoofing*, conforme já foi explicado, não consiste em um atentado às ferramentas utilizadas para proteger o dispositivo. Trata-se de uma técnica que se vale de brechas nos sistemas para acessar um dispositivo ou uma conta de serviços utilizados no ambiente cibernético.

Face ao exposto, considera-se a Lei nº 12.737/2012 uma norma penal em branco, conforme defendido por Sydow[590], cujo entendimento dos termos utilizados no texto legal será viabilizado por futuras definições. Essa espécie de norma foi mencionada pela primeira por Karl Binding, por volta do ano de 1870, quando estava trabalhando na elaboração do código penal da Alemanha. O art. 145 da referida legislação tipificava a desobediência das disposições sobre navegação, advindas do Imperador[591].

Ocorre que, à época da vigência do código citado, o Império Alemão era composto por vários reinos, cada um com sua própria legislação sobre questões aduaneiras, sendo assim preciso que houvesse uma penal única, cujas lacunas pudessem ser preenchidas de acordo com as normas locais. Essas leis penais foram denominadas de "leis de mandato em branco", tendo sido chamadas também de "normas cegas" e de "leis penais abertas"[592].

De acordo com uma frase atribuída a Binding, a norma penal em branco é "um corpo errante em busca de sua alma", ou seja, sem a complementação a norma não teria vigência no ordenamento jurídico[593]. Assim, nota-se que normas penais em branco são normas de composição imprecisa, pois descrevem uma conduta, porém a valoração da conjuntura fática que torna a conduta antijurídica depende de outra constante no próprio ordenamento jurídico[594].

---

[589] *Ibidem*, p. 300.
[590] *Ibidem, loc. cit.*
[591] RODRIGUES, Fabíola Emilin. **Tutela Penal Ambiental: Eficácia da Norma Penal em Branco**. Dissertação (Mestrado em Direito). Orientador: Marco Antonio Marques da Silva. Pontíficia Universidade Católica de São Paulo. São Paulo, 2005, p. 146.
[592] *Ibidem, loc. cit.*
[593] *Ibidem, loc. cit.*
[594] ALMEIDA, Bruno Torrano Amorim de. Controvérsias Atuais Acerca das Normas Penais em Branco. **Revista Jurídica Unicuritiba**, Curitiba, 2011, v. 26, n. 10, p. 38.

Trata-se de uma técnica legislativa, na qual a hipótese prevista em lei é elaborada de forma genérica, necessitando de outra lei, de cunho extrapenal, que viabilize a compreensão dos significados imprecisos do texto normativo. As leis penais em branco podem ser divididas entre próprias e impróprias. A primeira expressão refere-se às leis cujo complemento encontra-se em outra disposição legal emanada por uma instância legislativa distinta, enquanto a segunda designa a lei cuja complementação está prevista na mesma legislação ou em uma disposição legal emanada pela mesma instância legislativa[595].

Há três justificativas para a existência da norma penal em branco no âmbito de um ordenamento jurídico, de acordo com Vegas, citada por Rodrigues. Uma delas é a proteção de bens jurídicos complexos, pois a técnica utilizada na sua elaboração permite que outras entidades regulamentem tais matérias. Outro motivo é prevenir que a norma penal se torne obsoleta em virtude de novas questões decorrentes da evolução científica e social. Ademais, a norma penal em branco tem como um de seus objetivos equilibrar a relação entre tipicidade e legalidade por meio de um tipo penal menos inflexível[596].

A norma penal em branco não deixa de ser, assim, constitucional, mas, uma vez que a técnica para a criação de uma norma penal em branco tem como base a remissão, questiona-se quais seriam os critérios para que a norma incriminadora seja colmatada e se tais requisitos estão em conformidade com as normas que asseguram o Estado Democrático de Direito. Para tanto, é imprescindível que a norma penal em branco esteja em harmonia com os demais princípios previstos na Constituição[597].

Como falta ao legislador o conhecimento técnico necessário para elaboração do texto normativo, ele escolhe o bem jurídico que será salvaguardado pela norma penal em branco, deixando para as agências estatais a tarefa de regulamentar a matéria[598]. As agências do Estado possuem a credibilidade necessária para criar eventuais normas sobre questões de interesse público, constituindo, assim, a orientação necessária à norma penal em branco.

---

[595] PRADO, Luiz Regis. *Op. cit*., p. 199-200.
[596] VEGAS, Dulce María Santana. **El concepto de ley penal em blanco**. Buenos Aires: Editorial Ad-Hoc, 2000, p. 17 apud RODRIGUES, Fabíola Emilin. **Tutela Penal Ambiental: Eficácia da Norma Penal em Branco**. Dissertação (Mestrado em Direito). Orientador: Marco Antonio Marques da Silva. Pontíficia Universidade Católica de São Paulo. São Paulo, 2005, p. 154-155.
[597] RODRIGUES, Fabíola Emilin. **Tutela Penal Ambiental: Eficácia da Norma Penal em Branco**. Dissertação (Mestrado em Direito). Orientador: Marco Antonio Marques da Silva. Pontíficia Universidade Católica de São Paulo. São Paulo, 2005, p. 163-165.
[598] *Ibidem*, p. 47.

Como exemplo de uma situação assim, é possível mencionar a Lei nº 11.343/2006[599], a chamada Lei de Drogas, que depende de uma portaria da Agência Nacional de Vigilância Sanitária (Anvisa) para precisar a conceituação do termo "drogas".

Ocorre que, até o presente momento, não existe uma norma que especifique as expressões utilizadas na Lei de Crimes Informáticos. Conforme mencionado anteriormente, como o legislador não detém noções técnicas suficientes para elaborar determinados textos normativos e, no caso da Lei Carolina Dieckmann, não há menção a qualquer portaria de agência estatal que possa definir o significado de termos como "dispositivo informático" e "mecanismo de segurança".

Sobre a situação do acesso não autorizado aos smartphones das pessoas ligadas à Operação Lava Jato, uma vez que a conduta praticada pelos hackers não pode ser enquadrada no tipo previsto no 154-A do Código Penal por conta da primazia ao princípio da reserva legal, questiona-se se a referida ação poderia ser considerada um crime nos termos de outros artigos do referido diploma legal.

Pode-se fazer uma tentativa de compreensão da conduta à luz do então o tipo penal de violação de correspondência, previsto no seguinte artigo:

> **Violação de correspondência**
> **Art. 151 -** Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem:
> Pena - detenção, de um a seis meses, ou multa. Sonegação ou destruição de correspondência
> § 1º - Na mesma pena incorre:
> I - quem se apossa indevidamente de correspondência alheia, embora não fechada e, no todo ou em parte, a sonega ou destrói; Violação de comunicação telegráfica, radioelétrica ou telefônica;
> II - quem indevidamente divulga, transmite a outrem ou utiliza abusivamente comunicação telegráfica ou radioelétrica dirigida a terceiro, ou conversação telefônica entre outras pessoas;
> III - quem impede a comunicação ou a conversação referidas no número anterior; IV - quem instala ou utiliza estação ou aparelho radioelétrico, sem observância de disposição legal.
> § 2º - As penas aumentam-se de metade, se há dano para outrem.
> § 3º - Se o agente comete o crime, com abuso de função em serviço postal, telegráfico, radioelétrico ou telefônico:
> Pena - detenção, de um a três anos.
> § 4º - Somente se procede mediante representação, salvo nos casos do § 1º, IV, e do § 3º.

[599] BRASIL. **Lei nº 11.343** de 23 de agosto de 2006. Institui o Sistema Nacional de Políticas Públicas sobre Drogas - Sisnad; prescreve medidas para prevenção do uso indevido, atenção e reinserção social de usuários e dependentes de drogas; estabelece normas para repressão à produção não autorizada e ao tráfico ilícito de drogas; define crimes e dá outras providências.. Brasília, DF, 23 ago. 2006. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11343.htm. Acesso em: 27 mar. 2020.

Pela atual redação desse artigo, não se poderia considerar a violação de e-mail ou de mensagens trocadas por aplicativos como a conduta típica de violação de correspondência. Ocorre que o art. 10 da Lei n.º 9.296/96[600], a chamada Lei de Interceptação Telefônica, modificado recentemente pela Lei nº 13.869/2019[601], tipifica a conduta de interceptar comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.

A prática de *spoofing* para acessar um dispositivo informático alheio e, assim, obter acesso a mensagens trocadas por correio eletrônico ou por aplicativos pode ser considerada um crime nos termos do supramencionado artigo da Lei de Interpretações Telefônicas. Na referida hipótese está configurada uma interceptação de comunicação informática, flagrante violação à intimidade das pessoas que estão trocando mensagens.

Pergunta-se ainda se seria viável realizar uma interpretação lógico-sistemática, método interpretativo considerado de grande serventia para assegurar a unidade conceitual de todo o ordenamento jurídico, uma vez que apenas é possível chegar ao sentido de uma norma ao compreender o contexto normativo no qual ela está inserida[602]. Caso fosse empregado o método interpretativo lógico-sistemático, seria viável que o termo "correspondência" abrangesse comunicações informáticas, como mensagens de correio eletrônico e aplicativos, de forma que o uso do *spoofing* para ter acesso desautorizado a essas mensagens poderia ser considerado uma conduta criminosa, de acordo com o art.151 do Código Penal.

Contudo, se assim fosse, o princípio da legalidade seria desrespeitado. Ainda que já exista precedente na jurisprudência do Tribunal Superior do Trabalho sobre a legitimidade do monitoramento de e-mails corporativos por parte do empregador[603], considera-se que o

---

[600] BRASIL. **Lei nº 9.296**, de 24 de julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal. Brasília, DF, 24 jul. 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm. Acesso em: 28 mar. 2020.

[601] *Idem*. **Lei nº 13.869**, de 5 de setembro de 2019. Dispõe sobre os crimes de abuso de autoridade; altera a Lei nº 7.960, de 21 de dezembro de 1989, a Lei nº 9.296, de 24 de julho de 1996, a Lei nº 8.069, de 13 de julho de 1990, e a Lei nº 8.906, de 4 de julho de 1994; e revoga a Lei nº 4.898, de 9 de dezembro de 1965, e dispositivos do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal). Brasília, DF, 05 set. 2019. Disponível em http: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13869.htm#art41. Acesso em: 28 mar. 2020.

[602] BITENCOURT, Cezar Roberto. *Op. cit.*, p. 194.

[603] TRIBUNAL SUPERIOR DO TRABALHO. **Pode ou não Pode: O empregador monitorar e-mail corporativo de trabalhadores**. Disponível em: http://www.tst.jus.br/radio-destaques/-/asset_publisher/2bsB/content/pode-ou-nao-pode-o-empregador-monitorar-e-mail-corporativo-de-trabalhadores. Acesso em: 24 abr. 2020.

Código Penal brasileiro necessita urgentemente de uma reforma para incluir as correspondências eletrônicas no tipo previsto no retromencionado artigo.

Ademais, questiona-se se ação praticada pelas pessoas identificadas durante a Operação *Spoofing* poderia ser enquadrada no crime de divulgação de segredo, previsto no art. 153 do Código Penal. O tipo penal descreve como criminosa a conduta de divulgar sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor, e cuja divulgação possa produzir dano a outrem. Como já foi exposto, mensagens trocadas por aplicativos móveis não eram salvaguardadas pela legislação penal brasileira até a entrada em vigor da Lei nº 13.869/2019.

Entretanto, ainda há a indagação sobre o enquadramento do registro de troca de mensagens em aplicativos como "documento particular", outro termo contido no art. 153 do Código Penal. De acordo com o Dicionário Brasileiro da Língua Portuguesa Michaelis[604], a palavra "documento" diz respeito a qualquer escrito ou impresso que proporciona uma informação ou prova, podendo ser utilizado para esclarecimento de algo. Já o Dicionário Infopédia da Língua Portuguesa[605] explica que qualquer objeto elaborado com a finalidade de reproduzir ou representar uma pessoa, um facto, um dito ou um acontecimento pode ser considerado um documento.

Mensagens trocadas por aplicativos, assim, podem ser consideradas documentos, mesmo porque têm sido cada vez mais utilizadas como meios de prova em processos judiciais. Elas são consideradas, atualmente, como relevantes meios de convencimento do magistrado e comprovações das alegações das partes[606].

Conforme uma matéria disponibilizada no site da Revista Época, o uso do WhatsApp como meio de prova judicial é frequente nas mais diversas áreas, inclusive na criminal. A título de exemplo a matéria traz a informação de que, nos últimos dez anos, houve a publicação de noventa e nove acórdãos de segunda instância no Tribunal de Justiça do Rio de Janeiro (TJRJ)

---

[604] DOCUMENTO in **Dicionário Brasileiro da Língua Portuguesa Michaelis**. Disponível em: https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/documento/. Acesso em: 29 mar. 2020.

[605] DOCUMENTO in **Dicionário Infopédia da Língua Portuguesa**. Porto: Porto Editora, 2003-2020. Disponível em: https://www.infopedia.pt/dicionarios/lingua-portuguesa/documento. Acesso em: 29 mar. 2020.

[606] POLINARIO, Felipe Ramalho; MARTINI, Eduardo Giuntini. Utilização de mensagens e gravações em conversas de WhatsApp como meio de prova. **Jota**, 19 de outubro de 2019. Disponível em: https://www.jota.info/opiniao-e-analise/artigos/utilizacao-de-mensagens-e-gravacoes-em-conversas-de-whatsapp-como-meio-de-prova-19102019. Acesso em: 29 mar. 2020.

que registram a utilização das mensagens do aplicativo em processos por tráfico de drogas. Tal fato revela que a cada trinta e sete dias, em média, os desembargadores do TJRJ examinam textos, fotos, vídeos ou áudios enviados pelo WhatsApp e anexados aos autos dos processos como meios de prova[607].

A situação que motivou a Operação *Spoofing* poderia, dessa forma, ser encaixada no tipo penal descrito do art. 153 do Código Penal brasileiro. Trata-se de um caso em que os indivíduos detinham as mensagens, graças ao acesso viabilizado pelo *spoofing*, e divulgaram-nas, causando prejuízos às pessoas que tiveram suas contas de Telegram invadidas. No caso, o *spoofing* seria conduta preparatória e impunível, *ante facto* da divulgação.

Outra questão pendente, na análise da conjuntura dos fatos, seria a do termo "justa causa", contido no referido texto legal. O caso de hacktivismo foi uma violação à privacidade das pessoas envolvidas na Operação Lava Jato cujo aplicativo Telegram foi acessado em autorização. Por outro lado, supostas irregularidades nos procedimentos realizados durante a referida operação foram expostas[608], de modo que esse aspecto da "justa causa" ficaria a cargo do magistrado.

O desrespeito quanto à correspondência eletrônica, além de ser uma conduta mais sutil e furtiva do que a violação à correspondência física, o que dificulta sua descoberta e uma posterior denúncia, é ainda um problema para a legislação brasileira[609]. As leis que existem sobre a matéria ainda são escassas e pouco precisas quanto aos termos utilizados nos textos, bem como as decisões judiciais nesse sentido não são uniformes. O ordenamento jurídico brasileiro não está, até o presente momento, preparado para lidar com as características das relações desenvolvidas no ciberespaço, sendo essa uma situação que não pode permanecer ou não haverá segurança jurídica para a população em geral, uma vez que boa parte das pessoas utiliza meios informáticos para desempenhar as mais diversas atividades.

---

[607] MELLO, Bernardo. O Uso do WhatsApp como Prova na Justiça. **Revista Época**, 07 fev. 2020. Disponível em: https://epoca.globo.com/brasil/o-uso-do-whatsapp-como-prova-na-justica-24234263. Acesso em: 29 mar. 2020.

[608] GREENWALD, Glenn; GHIROTTO, Edoardo; MOLICA, Fernando; RESENDE, Leandro; PADUAN, Renata. Novos diálogos revelam que Moro orientava ilegalmente ações da Lava Jato. **Veja**, 12 jul. 2019. Disponível em: https://veja.abril.com.br/politica/dialogos-veja-capa-intercept-moro-dallagnol/. Acesso em: 29 mar. 2020.

[609] COELHO, Luiza Tângari. A Proteção da Intimidade na Correspondência Eletrônica: Extensão da Tutela da Correspondência Tradicional?. **Revista da Faculdade Direito da UFMG**. Belo Horizonte, 2012, n. 61,p. 369.

O desrespeito quanto à correspondência eletrônica, além de ser uma conduta mais sutil e furtiva do que a violação à correspondência física, o que dificulta sua descoberta e uma posterior denúncia, é ainda um problema para a legislação brasileira[610]. As leis que existem sobre a matéria ainda são escassas e pouco precisas quanto aos termos utilizados nos textos, bem como as decisões judiciais nesse sentido ainda não são uniformes. O ordenamento jurídico brasileiro não está, até o presente momento, preparado para lidar com as características das relações desenvolvidas no ciberespaço, sendo essa uma situação que não pode permanecer ou não haverá segurança jurídica para a população em geral, uma vez que boa parte das pessoas utiliza meios informáticos para desempenhar as mais diversas atividades.

Na redação do art. 154-A do Código Penal foi criado um tipo de invasão informática, que é mais restrito e, portanto, tem a aplicabilidade reduzida[611]. Na hipótese em que se configura a invasão informática ocorre um ataque a um sistema fechado, causando rupturas nos mecanismos de defesa, possibilitando o acesso desautorizado[612]. A intrusão informática, por sua vez, é uma expressão que abrange mais condutas. Nesse caso, o usuário desautorizado ingressa no sistema alheio valendo-se ou não de meios ardilosos ou violentos ou mesmo por meio de um subterfúgio para enganar o detentor dos direitos sobre o sistema. Pode ocorrer a obtenção de vantagem ilícita, porém trata-se de um aspecto dispensável para caracterizar a conduta de intrusão informática[613].

Para solucionar questões similares no futuro, o legislador poderia alterar, ou mesmo revogar, a Lei nº 12.737/2012 adotando um tipo penal similar ao previsto no art. 153 e no art. 153 bis do Código Penal Argentino[614]. De acordo com o texto desses artigos:

> **Articulo 153.** - Será reprimido con prisión de quince (15) días a seis (6) meses **el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido**; **o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida**.

[610] *Ibidem, loc. cit*.
[611] SYDOW, Spencer Toth. **Curso de Direito Penal Informático – Partes Geral e Especial.** Salvador: JusPodium, 2020, p. 438.
[612] SYDOW, Spencer Toth. **Crimes Informáticos e suas Vítimas.** São Paulo: Saraiva, 2ª ed., 2015, p. 114-115.
[613] *Ibidem*, p. 114.
[614] ARGENTINA. **Lei 11.179 (atualizada em 1984)**. Código Penal da Nação Argentina. Buenos Aires, 1984. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm. Acesso em: 27 mar. 2020.

> **En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.**
> La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.
> Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena. *(Artículo sustituido por art. 4° de la Ley N° 26.388, B.O. 25/6/2008)*
>
> **Articulo 153 bis.** - Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, **el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.**
> La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros. *(Artículo incorporado por art. 5° de la Ley N° 26.388, B.O. 25/6/2008)* **(Grifos nossos)**

O legislador argentino parece ter sido mais bem-sucedido na missão de proteger a privacidade do indivíduo do que o brasileiro. Ele não buscou regular a técnica utilizada para acessar indevidamente as mensagens trocadas no ciberespaço: simplesmente criminalizou o acesso sem autorização às referidas mensagens, não sendo relevante o meio empregado para fazê-lo. Em vez de mencionar expressões como "dispositivo informático" ou "mecanismo de segurança", termos que não foram esclarecidos o suficiente na Lei Carolina Dieckmann, o legislador usou vocábulos mais compreensíveis, como "comunicação eletrônica", "sem a devida autorização" e "sistema ou dado informático de acesso restringido".

Os bens jurídicos tutelados pela norma argentina são, segundo Aboso, o exercício individual da confidencialidade no trânsito das comunicações particulares, de natureza individual, e a liberdade de comunicação pessoal, tendo esse último um caráter mais difuso do que o primeiro. Ambos são considerados pelo autor como garantidores de uma das bases mais relevantes do Estado de Direito: a liberdade do indivíduo, o que significa que a todos os integrantes de uma comunidade deve ser garantido o direito de se comunicar livremente, ou seja, sem interferências. Isso contribui para o intercâmbio de ideias e, por conseguinte, viabiliza o processo democrático[615].

Um dos princípios normativos associados ao direito à comunicação é o direito à proteção constitucional da esfera privada, conforme destacam Barros e Oliveira[616]. Na mesma linha de

[615] ABOSO, Gustavo Eduardo. *Op. cit*., p. 154-155.
[616] BARROS, Bruno Mello Correa de.; OLIVEIRA, Rafael Santos de. A concentração midiática e o direito fundamental à comunicação no Brasil: perspectivas do cenário na sociedade em rede. **Cadernos de Direito**,

pensamento, Vannuchi[617] entende que a compreensão do direito à comunicação acarreta o reconhecimento de outros direitos, de modo que o aparato de proteção deve ser aperfeiçoado para coibir abusos como a violação do direito à privacidade, os crimes contra a honra e a exploração da imagem de crianças e vulneráveis.

Uma legislação adequada às demandas comunicacionais deve ser proporcionada pelos Estados aos indivíduos, pois o advento da sociedade da informação contribuiu para que as relações humanas estabelecessem o processo tecnológico como uma de suas bases. É preciso garantir, por meio de normas adequadamente elaboradas, que a troca de informações ocorra da maneira mais fluída possível[618].

No caso do Brasil, os legisladores, durante a concepção de normas voltadas para a regulação do ciberespaço, deveriam convocar os profissionais de Tecnologia da Informação e os juristas dedicados à área acadêmica para auxiliá-los nesse sentido. Dessa forma, seriam criadas leis mais eficientes e evitados problemas durante a aplicação dessas. Conforme já mencionado, não é aconselhável legislar sobre técnicas, como a "violação indevida de mecanismo de segurança" do art. 154-A, pois a mesma conduta pode ser praticada por diversas maneiras, tornado a legislação ineficaz. Ademais, termos imprecisos como "dispositivo informático" também dificultam a aplicação plena da norma.

No caso do *spoofing*, é o próprio titular do dispositivo ou da conta de e-mail/aplicativo que possibilita que outra pessoa acesse suas mensagens, não sendo possível considerar essa conduta uma "invasão" nos termos da Lei de Crimes Informáticos, pois não ocorre "violação indevida de mecanismo de segurança". Se o agente utilizasse algum *malware* para danificar os recursos de segurança do dispositivo e assim acessá-lo, então seria possível enquadrar a conduta no tipo penal previsto no art. 154-A, o que não ocorre com o emprego do método de *spoofing*.

Faz-se imprescindível respeitar o princípio da legalidade, uma técnica legislativa que visa impedir convenções penais arbitrárias e discriminatórias, bem como eliminar o uso de termos por demais vagos na legislação, tais como as expressões "socialmente perigosos" e "propensos a delinquir" [619]. O emprego de termos imprecisos como "dispositivos

---

Piracicaba, 2016, v. 16, p. 306.
[617] VANNUCHI, Camilo. O direito à comunicação e os desafios da regulação dos meios no Brasil. **Galaxia**, São Paulo, 2018, n. 38, p. 179.
[618] ABOSO, Gustavo Eduardo. *Op. cit*., p. 155.
[619] FERRAJOLI, Luigi. *Op. cit*., p. 35.

informáticos" e "violação de mecanismos de segurança" torna-se, assim, um obstáculo na aplicação da Lei Carolina Dieckmann.

O alcance garantista do convencionalismo penal está no entendimento simultaneamente nominalista e empirista da conduta punível, o que significa que somente as condutas taxativamente determinadas pela legislação podem ser consideradas criminosas, excluindo todas as demais do conceito de desvio passível de punição[620]. Dessa forma, não seria possível incluir o *spoofing* como método de "violação de mecanismo de segurança", pois o mesmo não causa qualquer tipo de prejuízo a essas ferramentas.

Ademais, o termo "dispositivo informático" não é abrangente o suficiente para proteger serviços utilizados apenas no ciberespaço, como contas de e-mail e aplicativos, uma vez que incluiria apenas aparelhos físicos, como, por exemplo, computadores e celulares. Em suma: a Lei nº 12.737/12 não é adequada para garantir a proteção os bens jurídicos, tais como a segurança informática e a privacidade, das pessoas que desempenham atividades no ciberespaço, por se tratar de uma norma penal em branco cuja aplicação pode acarretar um desrespeito ao princípio da reserva legal.

Entretanto, o acesso desautorizado a mensagens por meio de *spoofing* poderia ser encaixado no tipo penal previsto no art. 10º da Lei de Interceptação Telefônica. A técnica pode ser empregada para realizar a interceptação de comunicações informáticas, sendo considerada uma prática criminosa nos termos do citado artigo.

É ressaltado, mais uma vez, que o princípio da reserva legal possui, principalmente, uma essência política, uma vez que é a garantia fundamental da liberdade individual, que consiste em fazer apenas o que a lei permite. Somente a lei pode estabelecer os limites ao poder punitivo do Estado, caso contrário não haveria condições de garantir a segurança jurídica e, por conseguinte, a liberdade humana[621].

No caso do crime de invasão de dispositivo informático, é possível constatar que trata-se de uma lei penal em branco. Termos como "dispositivo informático" e "mecanismos de segurança" não estão suficientemente definidos no texto normativo do art. 154-A. Como não há, até o presente momento, um diploma normativo que especifique os significados dos termos retromencionados. Conforme explicado anteriormente, o *spoofing* não é um método

[620] *Ibidem, loc. cit.*
[621] JESUS, Damásio de. **Direito Penal: Parte Geral**, 21. ed. São Paulo: Saraiva, 1998, p. 61.

que viole ferramentas de segurança, mas uma forma de enganar o detentor do dispositivo informático para acessá-lo sem a sua devida autorização. Dessa forma, a conduta em questão não corresponde ao tipo penal descrito no art. 154-A do Código Penal.

O Estado moderno incluiu em seu ordenamento jurídico axiomas decorrentes do pensamento iluminista, de modo que seja estabelecido um modelo penal garantidor. Assim, não é admissível que o poder punitivo estatal seja exercido para castigar um indivíduo que praticou uma conduta não prevista na legislação penal. A hipótese de punir o indivíduo por conta do emprego do *spoofing*, sob a justificativa que tal conduta amolda-se à descrição do crime de invasão de dispositivo informático previsto no Código Penal brasileiro, trata-se de uma flagrante violação ao princípio da legalidade.

Caso essa situação efetivamente se concretize, entende-se que haverá um retrocesso em relação aos êxitos decorrentes da difusão da ideologia iluminista. O pensamento ilustrado é considerado um marco de extrema relevância, tanto que constitui um paradigma que, atualmente, permeia todas as legislações do mundo ocidental[622].

Uma vez que a intervenção estatal na esfera dos direitos do indivíduo para aplicar uma punição trata-se de uma forma opressão[623], não se pode deixar que esse poder sancionatório seja exercido de qualquer maneira. A observância do princípio da reserva legal deve ser realizada pelas autoridades públicas, mas não é possível que tal situação seja viabilizada quando a lei penal é por demais vaga, não apresentando termos que sejam precisos o suficiente para orientar o intérprete, como é o caso do art. 154-A do Código Penal brasileiro.

Conforme anteriormente destacado, as mudanças realizadas pela Lei nº 12.737/12 demonstraram uma maior preocupação do legislador sobre os meios empregados para violar os "dispositivos informáticos" do que com a conduta de "invasão" propriamente dita. Métodos que poderiam ser utilizados para acessar tais dispositivos, mas que não causam prejuízos às ferramentas de segurança, como o *spoofing*, não podem ser abarcados pelo art. 154-A. Assim, caso essa técnica fosse utilizada para obter acesso desautorizado a mensagens de aplicativos ou de e-mail, seria possível considerar que a conduta praticada corresponde somente ao crime de interceptação de comunicações informáticas, previsto no art. 10º da Lei nº 9.296/96, mas não ao crime de invasão de dispositivo informático.

---

[622] ARAÚJO, Fábio Roque. *Op. cit.*, p. 49.
[623] *Ibidem*, p. 55.

7 CONSIDERAÇÕES FINAIS

O Direito sofre modificações na medida em que a sociedade se torna mais complexa. O desenvolvimento da informática possibilitou muitas vantagens para a sociedade em geral, mas também tornou viáveis novas formas de cometimento de crimes. Fraudes praticadas por meios informáticos, acesso indevido a dispositivos da mesma natureza para obtenção de documentos particulares e material íntimo e divulgação não autorizada de informações privadas podem ser mencionados como comportamentos criminosos cada vez mais frequentes.

Mecanismos que, inicialmente, eram utilizados somente para intercâmbio e armazenamento de dados foram aperfeiçoados e tornados mais acessíveis, de modo que uma parte considerável da população mundial pode adquirir, por exemplo, um smartphone. Esse acesso, contudo, não está acompanhado de uma educação acerca dos riscos que a utilização desses dispositivos pode causar. Como boa parte das pessoas não tem dimensão suficiente de quais precauções devem ser tomadas nesse sentido, tornam-se vítimas em potencial para indivíduos que se valem desses meios para o cometimento de crimes.

A delinquência informática tem aspectos próprios que fazem dela mais desafiadora para as autoridades do que a criminalidade praticada no “mundo real”. Uma pessoa munida de um computador em um país pode acessar, de forma ilegal, dados que estão contidos em um sistema informático de outro e armazená-los em uma “nuvem” cuja empresa responsável está situada em um terceiro país. Trata-se de uma situação que requer a cooperação internacional de todos os países envolvidos, o que pode vir a ser ainda mais complicado devido ao grau de disparidade de recursos investidos na área de tecnologia da informação e à legislação vigente em cada um deles.

Dessa forma, os países estão se mobilizando para combater a criminalidade informática tanto por atuação em blocos, realizada por meio da assinatura de tratados, quanto por mudanças em suas legislações internas e realização de políticas nacionais para conscientizar e proteger a população dos riscos decorrentes do uso de ferramentas cibernéticas. Alguns países, por conta do nível de avanço tecnológico, já apresentam normas mais desenvolvidas nesse sentido, mas essa ainda não é a situação do Brasil.

Existe ainda um longo caminho a ser percorrido pelos legisladores e juristas no que tange ao combate à essa nova espécie criminalidade. Na criação do atual Código Penal, o legislador,

em virtude de uma impossibilidade histórica, não contemplou cenários nos quais é possível que uma pessoa instrua e comande um programa fora do território brasileiro para acessar material particular alheio armazenado em um computador, por exemplo. Trata-se de uma questão que ainda não encontra uma resposta específica no arcabouço normativo brasileiro.

No ciberespaço existem valores que ainda necessitam de uma proteção jurídica mais efetiva como, por exemplo, as ferramentas de acesso à rede; arquivos contendo textos e imagens e segurança na navegação pela Internet. Além disso, há outros bens jurídicos cuja violação também repercute no ciberespaço, como a honra e a intimidade, porém a sua salvaguarda ainda esbarra em questões burocráticas, como a falta de aparato legislativo e técnico. A maior parte das delegacias não possui o equipamento necessário, tampouco profissionais treinados, para investigar esse tipo de delito.

Embora já houvesse uma proposta legislativa com o intuito de dar uma resposta para a população acerca do crescente número de crimes informáticos, foi preciso que uma artista brasileira tivesse sua intimidade violada por indivíduos que acessaram seu computador sem autorização para obter dados particulares. Dessa forma, a Lei Carolina Dieckmann foi criada em 2012 para modificar o Código Penal e, desde sua entrada em vigor, tem sido aplicada para combater uma prática denominada “invasão de dispositivo informático”. A intenção do legislador foi a de preservar ferramentas informáticas e garantir a privacidade de seus usuários, medida de extrema relevância, considerando a quantidade crescente de casos nesse sentido.

A intimidade e a privacidade, bens jurídicos que, por vezes, são considerados sinônimos, são objetos de proteção de diversos ordenamentos jurídicos, como o americano, espanhol e brasileiro, conforme mencionado anteriormente nesse trabalho. Ocorre que o uso frequente de aparelhos informáticos e de ferramentas, como contas de e-mail e aplicativos, amplifica o risco de violações de materiais e informações particulares. É necessário então assegurar que tais bens jurídicos sejam preservados também no ciberespaço.

A Lei Carolina Dieckmann, dessa forma, trata-se de uma medida positiva do Poder Legislativo brasileiro em relação à salvaguarda da intimidade do indivíduo, compromisso firmado pelo Brasil em diversos tratados internacionais, sendo ainda um direito previsto na Constituição Federal como um direito fundamental da pessoa humana. É possível considerar que a criação desse novo dispositivo da legislação penal tem como finalidade a proteção de

um bem jurídico informa, que seria a segurança telemática, e a integridade e disponibilidade dos dados armazenados nos dispositivos informáticos.

Contudo, o tipo previsto no art. 154-A do Código Penal apresenta conceitos imprecisos, o que prejudica a sua aplicação. A referida norma não elucida expressões como "dispositivo informático" ou "mecanismo de segurança". Sobre o primeiro termo, o legislador não explica o que seria, tampouco buscou fazê-lo nos oito anos seguintes ao advento da Lei nº 12.737/2012.

Ademais, não se tem, até o momento, a definição do termo "mecanismo de segurança", de forma que é possível considerar o art. 154-A uma norma penal em branco. Dessa forma, será preciso uma outra norma para explicar o conceito de "dispositivo informático" e, até que esta seja elaborada, é possível que ocorram violações ao princípio da legalidade.

Assim sendo, as mais diversas técnicas podem ser empregadas para acessar um computador ou um smartphone, por exemplo, sem a autorização do seu titular. Um desse métodos é o *spoofing*, uma espécie de artifício utilizada para que o próprio detentor do aparelho ou da conta de e-mail/aplicativo viabilize o acesso para terceiros sem estar consciente disso.

Com o emprego de termos vagos no texto normativo, torna-se difícil a compreensão do objetivo do legislador. Infere-se que, durante o processo de elaboração do texto do art. 154-A do Código Penal, não houve participação de especialistas sobre o tema, como acadêmicos que se dediquem ao estudo do Direito Penal e de profissionais da área de Tecnologia da Informação, uma vez que os aspectos sobre a forma de cometimento do delito em questão foram ignorados.

No caso analisado, a conduta praticada pelos indivíduos, consistente no acesso desautorizado de contas de aplicativos pertencentes a funcionários públicos atuantes na Operação Lava Jato, não poderia ser considerada um crime nos termos do art. 154-A, pois o *spoofing* é uma técnica que não causa qualquer dano aos mecanismos de segurança que um smartphone possa ter, como um antivírus. Conforme explanado, trata-se de um ardil para enganar o titular da conta, com o intuito que ele possibilite o acesso. Na hipótese dessa conduta ser enquadrada no referido artigo, estaria configurada uma violação ao princípio da legalidade.

Para que situações como a retromencionada não se tornem empecilhos para que o Estado proteja a intimidade das pessoas, faz-se necessário que a legislação brasileira concernente ao

crime de invasão de dispositivo informático seja aperfeiçoada. De acordo com o conteúdo já explanado, é preciso que se legisle sobre condutas e não sobre técnicas, uma vez que as últimas podem ser alteradas mais frequentemente, tornando a norma obsoleta em pouco tempo ou até mesmo antes de sua entrada em vigor.

Caso o *spoofing* fosse utilizado no momento atual para acesso indevido a uma conta de e-mail ou de aplicativo, a prática em questão não deveria ser enquadrada no art. 154-A do Código Penal, mas no art. 10 da Lei nº 9.296/1996, recentemente modificado pela Lei nº 13.964/2019, que passou a tipificar a interceptação de comunicações telemáticas sem autorização judicial ou com objetivos não autorizados em lei. A conduta não poderia se adequar ao tipo penal previsto no artigo criado pela Lei Carolina Dieckmann, pois uma conta de e-mail ou aplicativo não poderia ser considerada um "dispositivo informático" e tampouco se trata de uma invasão informática, uma vez que não foram causados danos ao sistema de segurança do dispositivo.

A legislação brasileira voltada ao combater à criminalidade informática ainda não está amadurecida o suficiente para dar uma resposta satisfatória a esse problema. A elaboração de normas eficientes nesse sentido deve ser um processo criativo de uma equipe multidisciplinar, envolvendo profissionais de áreas como Direito, Tecnologia da Informação e Comunicação, de modo que as leis sobre crimes informáticos não necessitem ser alteradas constantemente, em virtude de novas técnicas informáticas desenvolvidas. Assim, situações que acarretem insegurança jurídica serão evitadas por meio de normas que proporcionem tanto a salvaguarda da intimidade e da privacidade e, simultaneamente, estejam de acordo com os princípios basilares do Estado de Direito.

REFERÊNCIAS

ABOSO, Gustavo Eduardo. Derecho Penal Cibernético: **La Ciber criminalidade y el Derecho penal em la moderna sociedad de la información y la tecnologia de la comunicación**, Buenos Aires: Editorial B de F, 2017.

ABUKHATER, Shaima. The Impact of the Applicability of Social Media and Social Networking Sites on Business Firms' Effectiveness and Profit Field Study: Telecommunication Sector in Jordan. **International Journal of Managerial Studies and Research (IJMSR)**, Ongole, jun 2015, Volume 3, Issue 6, p. 153-164.

ALBIACH, Juan Pardo. Ciberacoso: Cyberbullying, Grooming, Redes Sociales y Otros Perigos. In: GONZÁLEZ, Javier García (Coordenador). **Ciberacoso: la tutela penal de la**

intimidad, la integridad y la libertad sexual em Internet. Valencia: Tirant Lo Blanch, 2010, p. 51-83.

ALEMANHA. **Bundeslagebilder Cybercrime**, 2018. Disponível em: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/cybercrime_node.html. Acesso em: 24 fev. 2020.

ALEMANHA, **Constituição da República Federal da Alemanha**. Bonn, 23 maio de 1949. Disponível em: https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html. Acesso em: 15 mar. 2020.

ALEMANHA. **Código Penal Alemão**. Berlin, 13 de novembro de 1998. Disponível em: https://www.gesetze-im-internet.de/stgb/. Acesso em: 24 fev. 2020.

ALEMANHA. **Strafgesetzbuch**, 15 maio 1871. Disponível em: https://www.gesetze-im-internet.de/stgb/. Acesso em: 24 fev. 2020.

ALEMANHA. **Zweites Gesetz Bekämpfung der Wirtschaftskriminalität**. Bonn, 23 de maio 1986. Disponível em:https://www.bgbl.de/xaver/bgbl/text.xav?SID=&tf=xaver.component.Text_0&tocf=&qmf=&hlf=xaver.component.Hitlist_0&bk=bgbl&start=%2F%2F*%5B%40node_id%3D%27379873%27%5D&skin=pdf&tlevel=-2&nohist=1. Acesso em: 24 fev. 2020.

ALMEIDA, Bruno Torrano Amorim de. Controvérsias Atuais Acerca das Normas Penais em Branco. **Revista Jurídica Unicuritiba**. Curitiba, 2011, v. 26, n. 10, p. 36-69.

ALVES, Paulo. **O que é Spoofing? Técnica foi usada para hackear Sergio Moro, diz polícia.** Disponível em: https://www.techtudo.com.br/noticias/2019/07/o-que-e-spoofing-tecnica-foi-usada-para-hackear-sergio-moro-diz-policia.ghtml. Acesso em: 23 ago. 2019.

ANTUNES, Mário; RODRIGUES, Baltazar. **Introdução à Cibersegurança: A Internet, os Aspectos Legais e a Análise Digital Forense.** Lisboa: FCA – Editora de Informática Ltda, 2018.

AOS 19 anos, o argentino Santiago López fez história: é o primeiro "hacker ético" a atingir a quantia de US$ 1 milhão, o equivalente a R$ 3,8 milhões, descobrindo erros de informação. **BBC**, 05 mar. 2019. Disponível em: https://www.bbc.com/portuguese/internacional-47423964. Acesso em: 29 jan. 2020.

ARAS, Vladimir. Videoconferência no Processo Penal. **Boletim Científico da Escola Superior do Ministério Público da União**. Brasília, abr./jun. 2005, n.15, p. 173-195.

ARGENTINA. **Lei 11.179** (atualizada em 1984). Código Penal da Nação Argentina. Buenos Aires, 1984. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm. Acesso em: 27 mar. 2020.

ARGENTINA. **Lei 26.388**, de 24 de junho de 2008. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm. Acesso em: 26 fev. 2020.

ARGENTINA. **Lei 26.904**, 04 de dezembro de 2013. Disponível em: http://servicios.infoleg.gob.ar/infolegInternet/anexos/220000-224999/223586/norma.htm. Acesso em: 26 fev. 2020.

ARGENTINA. **Lei 27.436**, 21 de março de 2018. Disponível em: https://www.argentina.gob.ar/normativa/nacional/ley-27436-309201. Acesso em: 26 fev. 2020.

ARGENTINA. **Resolución Ministerial 69/16** - Creación del Programa Nacional Contra la Criminalidad Informática en la órbita del Ministerio de Justicia, 11 de marzo de 2016. Disponível em: http://www.saij.gob.ar/creacion-programa-nacional-contra-criminalidad-informatica-orbita-ministerio-justicia-nv14027-2016-03-11/123456789-0abc-720-41ti-lpssedadevon. Acesso em: 26 fev. 2020.

ÁVILA, Ana Paula Oliveira; WOLOSZYN, André Luis. A tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência. **Revista de Investigações Constitucionais**, Curitiba, set/dez. 2017, v. 4, n. 3, p. 167-200.

ARAÚJO, Fábio Roque. **O princípio da proporcionalidade referido ao legislador penal.** Salvador: Faculdade Baiana de Direito, 2011.

ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**. Paris, 1948. Disponível em: https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por. Acesso em: 20 set. 2019.

ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS. **Pacto Internacional sobre Direitos Civis e Políticos**. Nova York, 1966. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm. Acesso em: 20 set. 2019.

BACH, Sirlei Lourdes. **Contribuição do Hacker para o Desenvolvimento Tecnológico da Informática**. Dissertação. Programa de Pós-graduação em Tecnologia da Informação. Universidade Federal de Santa Catarina. 2001. Disponível em: https://repositorio.ufsc.br/xmlui/handle/123456789/82176. Acesso em: 08 ago. 2019.

BARATT, Monica J.; ALDRIDGE, Judith; MADDOX, Alexia. **The SAGE Encyclopedia of the Internet.** Thousand Oaks: SAGE Publications Inc., 2018.

BARNES, Julian E.; SANGER, David E. Congress, Warning of Cybersecurity Vulnerabilities, Recommends Overhaul. **New York Times**, 11 mar. 2020. Disponível em: https://www.nytimes.com/2020/03/11/us/politics/congress-cyber-solarium.html. Acesso em: 22 fev. 2020.

BARRANCO, Norberto J. de la Mata. La Tutela de la Integridad y Disponibilidad de Datos y Sistemas Informáticos: el Modelo Tradicional Vinculado a uma Protección Estrictamente Patrimonisl, um Mal Referente. In: RIQUERT, Marcelo A. (direção); SUEIRO, Carlos Christian (coordenação). **Sistema penal e informática: ciberdelitos, evidencia digital, TICS**. Buenos Aires: Hammurabi, 2019, p. 29-49.

BARRIO, Laura. Exposição de conteúdo erótico na internet vira crime contra a dignidade sexual. **Agência Universitária de Notícias da USP**, 13 fev. 2019. Disponível em: https://paineira.usp.br/aun/index.php/2019/02/13/exposicao-de-conteudo-erotico-na-internet-vira-crime-contra-a-dignidade-sexual/. Acesso em: 18 fev. 2020.

BARROS, Bruno Mello Correa de.; OLIVEIRA, Rafael Santos de. A concentração midiática e o direito fundamental à comunicação no Brasil: perspectivas do cenário na sociedade em rede. **Cadernos de Direito**. Piracicaba, 2016, v. 16, p. 293-329.

BARROS FILHO, Clóvis de.; PERES NETO, Luiz. Éticas em rede: pautas para a luta contra a pornografia infantil e os delitos de ódio nos sites de redes sociais. In: BRASIL. Ministério Público Federal. **Crimes Cibernéticos: Coletânea de Artigos**, 2018, v. 3, p. 184-197.

BBC News launches 'dark web' Tor Mirror. **BBC**, 23 out. 2019. Disponível em: https://www.bbc.com/news/technology-50150981. Acesso em: 11 fev. 2020.

BECK, Ulrich. **Sociedade de Risco: Rumo a uma outra modernidade**. São Paulo: Ed. 44, 2010.

BERGMAN, Michael K. **The Deep Web: Surfacing Hidden Value**. Sioux Falls: Bright Planet, 2001.

BERKELEY, Istvan S. N. A Computational Conundrum: "What is a Computer?" A Historical Overview. **Minds and Machines**, 2018, v. 28, p. 375–383.

BIDASOLO, Mirentxu Corcoy. Prólogo. In ABOSO, Gustavo Eduardo. **Derecho Penal Cibernético: La cibercriminalidade y el Derecho penal em la moderna sociedad de la información y la tecnologia de la comunicación**, Buenos Aires: Editorial B de F, 2017, p. XXI-XXIII.

BIGONHA, Carolina. Inteligência Artificial em perspectiva. **Panorama Setorial**. São Paulo, out. 2018, ano 10, n. 2, p. 1-16.

BITENCOURT, Cezar Roberto. **Tratado de Direito Penal**. São Paulo: Saraiva, 10a ed., 2006.

BRASIL. **Caso Lava Jato**. Ministério Público Federal. Disponível em: http://www.mpf.mp.br/grandes-casos/lava-jato. Acesso em: 01 mar. 2020.

BRASIL. Conselho da Europa convida o Brasil para compor a Convenção de Budapeste sobre o Cibercrime. **Ministério Público Federal**, 13 dez. 2019. Disponível em http://www.mpf.mp.br/pgr/noticias-pgr/conselho-da-europa-convida-o-brasil-para-compor-a-convencao-de-budapeste-sobre-o-cibercrime. Acesso em: 13 mar. 2020.

BRASIL. **Constituição da República Federativa do Brasil**. Brasília, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 20 set. 2019.

BRASIL. **Decreto nº 678**, de 6 de novembro de 1992. Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 06 de novembro de 1992.

Brasília, DF, 25 set. 1992. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/D3468.htm. Acesso em: 17 mar. 2020.

BRASIL. **Decreto nº 3.468**, de 17 maio 2000**.** Promulga o Protocolo de Assistência Jurídica Mútua em Assuntos Penais, assinado em San Luis, República Argentina, em 25 de junho de 1996, entre os Governos da República Federativa do Brasil, da República Argentina, da República do Paraguai e da República Oriental do Uruguai. Brasília, DF, 17 maio de 2000. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/D3468.htm. Acesso em: 22 fev. 2020.

BRASIL. **Decreto nº 7.158**, de 20 de abril de 2010. Autoriza a Secretaria de Direitos Humanos da Presidência da República a dar cumprimento a sentença exarada pela Corte Interamericana de Direitos Humanos. Brasília, DF, 20 abr. de 2010. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2007-2010/2010/decreto/D7158.htm. Acesso em: 17 mar. 2020.

BRASIL. **Decreto-lei nº 1.004**, de 21 de outubro de 1969. Código Penal. Brasília, DF, 21 out. 1969. Disponível em http://www.planalto.gov.br/ccivil_03/Decreto-Lei/1965-1988/Del1004.htm. Acesso em: 20 mar. 2020.

BRASIL. **Decreto-lei nº 2.848**, de 7 de dezembro de 1940. Código Penal. Brasília, DF, 7 dez. 1940. Disponível em http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm. Acesso em: 20 set. 2019.

BRASIL. Em conferência internacional, MPF defende cooperação como forma de combater o cibercrime. Ministério Público Federal. **Ministério Público Federal**. 14 mar. 2018. Disponível em http://www.mpf.mp.br/pgr/noticias-pgr/em-conferencia-internacional-mpf-defende-cooperacao-como-forma-de-combater-o-cibercrime. Acesso em: 15 mar. 2020.

BRASIL. **Emenda constitucional nº 45**, de 30 de dezembro de 2004. Altera dispositivos dos arts. 5º, 36, 52, 92, 93, 95, 98, 99, 102, 103, 104, 105, 107, 109, 111, 112, 114, 115, 125, 126, 127, 128, 129, 134 e 168 da Constituição Federal, e acrescenta os arts. 103-A, 103B, 111-A e 130-A, e dá outras providências. Brasília, DF, 30 dez. 2004. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc45.htm. Acesso em: 17 mar. 2020.

BRASIL. Juiza quer desabilitar criptografia de suspeitos no Whatsapp; entenda. **Empresa Brasileira de Comunicação**, 19 jul. 2016. Disponível em: http://www.ebc.com.br/tecnologia/2016/07/juiza-quer-desabilitar-criptografia-no-whatsapp-entenda. Acesso em: 13 mar. 2020.

BRASIL. **Lei nº 7.170**, de 14 de dezembro de 1983. Define os crimes contra a segurança nacional, a ordem política e social, estabelece seu processo e julgamento e dá outras providências. Brasília, DF, 14 dez. de 1983. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l7170.htm. Acesso em: 19 out. 2020.

BRASIL. **Lei nº 8.069**, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF, 13 jul. de 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 17 fev. 2020.

BRASIL. **Lei nº 9.296**, de julho de 1996. Regulamenta o inciso XII, parte final do artigo 5º da Constituição Federal. Brasília, DF, 24 jul. 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/LEIS/L9296.htm. Acesso em: 21 set. 2019.

BRASIL. **Lei nº 10.406**, de 10 de janeiro de 2002. Institui o Código Civil. Brasília, DF, 10 jan. 2002. Disponível em http://www.planalto.gov.br/ccivil_03/LEIS/2002/L10406.htm. Acesso em: 20 set. 2019.

BRASIL. **Lei nº 11.343**, de 23 de agosto de 2006. Institui o Sistema Nacional de Políticas Públicas sobre Drogas - Sisnad; prescreve medidas para prevenção do uso indevido, atenção e reinserção social de usuários e dependentes de drogas; estabelece normas para repressão à produção não autorizada e ao tráfico ilícito de drogas; define crimes e dá outras providências. Brasília, DF, 23 ago. 2006. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11343.htm. Acesso em: 16 fev. 2020.

BRASIL. **Lei nº 12.735**, de 30 de novembro de 2012. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Brasília, DF, 30 nov. de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm. Acesso em: 04 fev. 2020.

BRASIL. **Lei nº 12.737**, de 30 de novembro de 2012**.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.. Brasília, DF, 30 nov. de 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em: 04 fev. 2020.

BRASIL. **Lei nº 12.965**, de 23 de abril de 2014. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.. Brasília, DF, 23 abr. de 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 04 fev. 2020.

BRASIL. **Lei nº 13.185**, de 06 de novembro de 2015. Institui o Programa de Combate à Intimidação Sistemática (Bullying). Brasília, DF, 06 nov. 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13185.htm. Acesso em: 18 fev. 2020.

BRASIL. **Lei nº 13.260**, de 16 de março de 2016. Regulamenta o disposto no inciso XLIII do art. 5º da Constituição Federal, disciplinando o terrorismo, tratando de disposições investigatórias e processuais e reformulando o conceito de organização terrorista; e altera as Leis n º 7.960, de 21 de dezembro de 1989, e 12.850, de 2 de agosto de 2013. Brasília, DF, 16 mar. 2016. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13260.htm. Acesso em: 19 out. 2020.

BRASIL. **Lei nº 13.709**, de 14 de agosto de 2018. Brasília, DF, 19 dez. 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 14 ago. 2018. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 10 fev. 2020.

BRASIL. **Lei nº 13.772**, de 19 de dezembro de 2018. Altera a Lei nº 11.340, de 7 de agosto de 2006 (Lei Maria da Penha), e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), para reconhecer que a violação da intimidade da mulher configura violência doméstica e familiar e para criminalizar o registro não autorizado de conteúdo com cena de nudez ou ato sexual ou libidinoso de caráter íntimo e privado. Brasília, DF, 19 dez. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13772.htm. Acesso em: 21 set. 2019.

BRASIL. **Lei nº 13.834**, de 04 de junho de 2019. Altera a Lei nº 4.737, de 15 de julho de 1965 - Código Eleitoral, para tipificar o crime de denunciação caluniosa com finalidade eleitoral. Brasília, DF, 04 jun. 2019. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/L13834.htm. Acesso em: 18 fev. 2020.

BRASIL. **Projeto de Lei 2857/19.** Altera a Lei no 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para estabelecer aumento da pena ao crime de aliciamento de crianças e adolescentes pelo uso de aplicativo de comunicação via internet. Brasília, DF, 14 maio 2019. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=43018290D54FE7EA03EF2C2B6F7DC3F2.proposicoesWebExterno2?codteor=1747399&filename=PL+2857/2019. Acesso em: 17 fev. 2020.

CAMAROTTO, Murillo; MARTINS, Luísa; PERON, Isadora. Glenn Greenwald é denunciado junto com hackers na Operação Spoofing. **Valor**. Brasília, 21 jan. 2020. Disponível em: https://valor.globo.com/politica/noticia/2020/01/21/glenn-greenwald-e-denunciado-junto-com-*hackers*-na-operacao-spoofing.ghtml. Acesso em: 01 mar. 2020.

CARVALHO, Ivan Lira de. **Crimes na Internet: há como puni-los**. Jus.com.br, out. 2001. Disponível em: https://jus.com.br/artigos/2081/crimes-na-internet. Acesso em: 04 fev. 2020.

CARVALHO, Luis Gustavo Grandinetti Castanho de. Direito à privacidade. **Revista da EMERJ**. Rio de Janeiro, 1998, v. 1, n. 2, p. 51-76.

CASTELLS, Manuel. **A Sociedade em Rede – Volume 1**, 8ª ed., São Paulo: Paz e Terra, 2005.

CASTRO, Leonardo Bellini de. As Implicações Jurídico-Constitucionais da Tutela da Intimidade e suas Relações com a Atividade Investigatória do Estado. **Revista Jurídica ESMP-SP**. São Paulo, 2013, v. 4, p. 59-84.

CASTRO, Luiz Felipe. O Snowden da Bola: Quem é o hacker português por trás do Football Leaks, o vazamento de milhões de documentos sigilosos que revelou negociatas e falcatruas dentro e fora dos gramados. **Veja**, São Paulo, ed. 2675, ano 53, n. 9, 26 fev. 2020, p. 78-79.

CHERÑAVSKY, Nora; MUNIAGURRIA, Pablo Gris; MOREIRA, Diógenes. A diez años de la Ley de Delitos Informáticos. Balance y Propuestas. In: In: RIQUERT, Marcelo A.

(direção); SUEIRO, Carlos Christian (coordenação). **Sistema penal e informática: ciberdelitos, evidencia digital, TICS**. Buenos Aires: Hammurabi, 2019, p. 129-160.

CHILE. **Ley 19.223,** de 7 de junio de 1993. Disponível em: https://www.leychile.cl/Navegar?idNorma=30590. Acesso em: 26 fev. 2020.

CLARK, David. **Characterizing cyberspace: past, present and future**. 2010. Disponível em: https://projects.csail.mit.edu/ecir/wiki/images/7/77/Clark_Characterizing_cyberspace_1-2r.pdf. Acesso em: 27 dez. 2019.

CÓ, Pedro Rosa. Artigo 66: Protocolos ou acordos particulares poderão completar, em caso de necessidade, as disposições da presente Carta. In: JERÓNIMO, Patrícia; GARRIDO, Rui; PEREIRA, Maria de Assunção do Vale. **Comentário Lusófono à Carta Africana dos Direitos Humanos e dos Povos**. Braga: Observatório Lusófono dos Direitos Humanos da Universidade do Minho (OLDHUM), 2018, p. 533-560.

COELHO, Luiza Tângari. A Proteção da Intimidade na Correspondência Eletrônica: Extensão da Tutela da Correspondência Tradicional? **Revista da Faculdade Direito da UFMG**. Belo Horizonte, 2012, n. 61, p. 355-395.

COHEN-ALMAGOR, Raphael. Internet History. **International Journal of Technoethics**, 2011, v. 2, n. 2, p. 45-64.

COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS. **Convenção Americana sobre Direitos Humanos**. San José, 1969. Disponível em: https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm. Acesso em: 20 set. 2019.

CONTRACT FOR THE WEB. **A global plan of action to make our online world safe and empowering for everyone**. Disponível em: https://contractfortheweb.org/. Acesso em: 12 mar. 2020.

CONSELHO DA EUROPA. **Convenção sobre o Cibercrime.** Budapeste, 23 nov. 2001. Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf. Acesso em: 17 fev. 2020.

CONSELHO DA EUROPA. **Convenção Europeia dos Direitos Humanos**. Roma, 4 nov. 1950. Disponível em: https://www.echr.coe.int/Documents/Convention_POR.pdf. Acesso em: 14 mar. 2020.

CORDEIRO, Edmar Lima. Direito à Privacidade de Informação. **Revista de Ciências Jurídicas e Sociais da UNOPAR**. Toledo, 2001, v. 4, p. 5-24.

CORTE INTERAMERICANA DE DIREITOS HUMANOS. **Caso Escher e Outros vs. Brasil**. Washington, 06 de julho de 2009. Disponível em http://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf. Acesso em: 17 mar. 2020.

CORTE INTERAMERICANA DE DIREITOS HUMANOS. **Fontevecchia y D'amico Vs. Argentina**. Washington, 29 nov. 2011. Disponível em: http://www.corteidh.or.cr/CF/jurisprudencia2/ficha_tecnica.cfm?nId_Ficha=191. Acesso em: 17 mar. 2020.

COSTA JÚNIOR, Paulo José da. **O Direito de Estar Só: A tutela Penal do direito à intimidade**, 3a ed. São Paulo: Siciliano Jurídico

COUNCIL OF EUROPE. **Chart of signatures and ratifications of Treaty - Convention on Cybercrime**. Disponível em: https://www.coe.int/en/web/conventions/full-list/ /conventions/treaty/185/signatures?p_auth=exhG7iJ7. Acesso em: 23 fev. 2020.

COUNCIL OF EUROPE. **Global Project Cybercrime@Octopus**. Disponivel em: https://www.coe.int/en/web/cybercrime/cybercrime-octopus. Acesso em: 24 fev. 2020.

COUNCIL OF EUROPE. **US support to the Budapest Convention**. Estrasburgo, 25 set. 2018. Disponível em: https://www.coe.int/en/web/cybercrime/-/us-support-to-the-budapest-convention. Acesso em: 24 fev. 2020.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Editora Saraiva, 2011.

CRESPO, Marcelo Xavier de Freitas. Sobre o acesso a dispositivos digitais sem autorização judicial em situações de flagrante delito. In: PINHEIRO, Patrícia Peck. **Direito Digital 3.0 Aplicado**. São Paulo: Thompson Reuters, 2018, p. 88-110.

CRIMES cibernéticos disparam e expõem fragilidade tecnológica no Brasil. **Estado de Minas**, Belo Horizonte, 04 ago. 2019. Disponível em: https://www.em.com.br/app/noticia/politica/2019/08/04/interna_politica,1074689/crimes-ciberneticos-disparam-expoem-fragilidade-tecnologica-no-brasil.shtml. Acesso em: 13 abr. 2020.

CRIMES cibernéticos: descubra como você pode se proteger de ataques na internet. **Agência Nacional de Telecomunicações**, 27 ago. 2019. Disponível em . Acesso em: 13 abr. 2020.

DATASAFER. 30.389 atendimentos e 4.134.808 denúncias. **SaferNet**. Disponível em: https://indicadores.safernet.org.br/indicadores.html. Acesso em: 18 maio 2020.

DAVIS, Jeremy Seth. German police coordinate with Europol to nab DroidJack useres. **SC Magazine**, 30 out. 2015. Disponível em: https://www.scmagazine.com/home/security-news/german-police-coordinate-with-europol-to-nab-droidjack-users/. Acesso em: 16 mar. 2020.

DECISÃO de juiz do Piauí manda tirar WhatsApp do ar em todo o Brasil. **G1**, Teresina, 25 fev. 2015. Disponível em: http://g1.globo.com/pi/piaui/noticia/2015/02/decisao-de-juiz-do-piaui-manda-tirar-whatsapp-do-ar-em-todo-o-brasil.html. Acesso em: 12 mar. 2020.

DELEGACIAS Cibercrimes. **SaferNet**. Disponível em: https://new.safernet.org.br/content/delegacias-cibercrimes. Acesso em: 13 abr. 2020.

DELUCA, Santiago; DEL CARRIL, Enrique. Cooperación Internacional en Materia Penal en el Mercosur: el Cibercrimen. **Revista da Secretaria do Tribunal Permanente de Revisão**. Assunção, out. 2017, ano 5, n. 10, p. 13-28.

DE LUCA, Javier Augusto; LUZZA, Yamila Yael. "Fake News": Cibercriminalidad y Libertad de Expresión em Internet. In: RIQUERT, Marcelo A. (direção); SUEIRO, Carlos Christian (coordenação). **Sistema penal e informática: ciberdelitos, evidencia digital, TICS**. Buenos Aires: Hammurabi, 2019, p. 51-71.

DEL CARRIL, Enrique H. del. Desafíos del Cibercrimen Para el Derecho Internacional. In: DUPUY, Daniela (Direção); KIEFER, Mariana (Coordenação). **Cibercrimen II: Nuevas conductas penales y contravencionales; Inteligencia artificial aplicada al Derecho Penal y procesal penal; Novedosos médios probatórios para recolectar evidencia digital; Cooperación internacional y victimología**. Buenos Aires: Editorial B de F, 2018, p. 383-402.

DENÚNCIAS de crimes online contra mulheres sobem 1600% no Brasil em 2018. **Revista Painel Político**, 07 de fev. 2019. Disponível em: https://revista.painelpolitico.com/denuncias-de-crimes-online-contra-mulheres-sobem-1600-no-brasil-em-2018/. Acesso em: 13 mar. 2020.

DIAZ, Pedro Vidal. **DEVIR-HACKER: Empirismo, Ética e Ontologia na Era Informacional**. Dissertação (Mestrado em Ciência da Informação). Escola de Comunicação da Universidade Federal do Rio de Janeiro. 2017, 158 fls. Disponível em http://ridi.ibict.br/bitstream/123456789/959/1/IBICT_Pedro_DIAZ_Dissertacao_Mestrado_.p.pdf. Acesso em: 17 jan. 2020.

DIECKMANN é assunto mais falado do Twitter após vazamento de fotos. **G1**, 04 maio 2012. Disponível em: http://g1.globo.com/tecnologia/noticia/2012/05/dieckman-e-assunto-mais-falado-do-twitter-apos-vazamento-de-fotos.html. Acesso em: 01 mar. 2020.

DIFFERENCE between Phishing and Spoofing. **TechDifferences**, 01 fev. 2018. Disponível em: https://techdifferences.com/difference-between-phishing-and-spoofing.html. Acesso em: 16 fev. 2020.

DIGITAL DETOX. In: **Lexico: Powered by Oxford**. Disponível em: https://www.lexico.com/definition/digital_detox. Acesso em: 04 mar. 2020.

DUPUY, Daniela; KIEFER, Mariana. La Nueva Ley "*Cloud Act*" su Impacto em Investigaciones en Entornos Digitales. In: In: RIQUERT, Marcelo A. (direção); SUEIRO, Carlos Christian (coordenação). **Sistema penal e informático: ciberdelitos, evidencia digital, TICS**. Buenos Aires: Hammurabi, 2019, p. 219-236.

DURÃES, Cintya Nishimura; LEÃO JUNIOR, Teofilo Marcelo de Area; SANCHES, Raquel Cristina Ferraroni. Tutela do Direito à Intimidade. **Revista Eletrônica de Graduação do UNIVEM [REGRAD]**. Marília, 2014, n. 1, p. 73-102.

ESPANHA. **Ley Orgánica 10/1995**, de 23 de noviembre, el Código Penal. Disponível em: https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444. Acesso em 24 fev. 2020.

ESTADOS UNIDOS. **Cybersecurity and Privacy**. Departamento de Segurança Interna. Disponível em: https://www.dhs.gov/cybersecurity-and-privacy. Acesso em 17 mar. 2020.

ESTADOS UNIDOS. New York Civil Rights Law, abr.1903, **Laws of the State of New York Passed at the Sessions of the Legislature**, 1903, v. 01. Disponível em: https://babel.hathitrust.org/cgi/pt?id=nyp.33433090742549&view=1up&seq=320. Acesso em: 09 mar. 2020.

ESTADOS UNIDOS. Quarta Emenda à Constituição. **United States Courts**. Disponível em: https://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0. Acesso em: 07 mar. 2020.

FELITTI, Guilherme. Por que as operadoras brasileiras entraram em guerra contra o WhatsApp. **Época Negócios**, 16 dez. 2015. Disponível em: https://epocanegocios.globo.com/Informacao/Dilemas/noticia/2015/12/por-que-operadoras-brasileiras-entraram-em-guerra-contra-o-whatsapp.html. Acesso em: 23 dez. 2019.

FERREYRA, Eduardo. Uma visión desde los derechos humanos sobre las tecnologias de vigilância e investigación. In: RIQUERT, Marcelo A. (direção); SUEIRO, Carlos Christian (coordenação). **Sistema penal e informática: ciberdelitos, evidencia digital - TICS**. Buenos Aires: Hammurabi, 2019, p. 113-126.

FERNANDES. Augusto. Crimes virtuais e ataques cibernéticos mais do que dobram em um ano. **Correio Braziliense**, Brasília, 04 de agosto de 2019. Disponível em: https://www.correiobraziliense.com.br/app/noticia/politica/2019/08/04/interna_politica,775357/crimes-virtuais-e-ataques-ciberneticos-mais-do-que-dobram-em-um-ano.shtml. Acesso em 13 abr. 2020.

FERNÁNDEZ, David Lorenzo Morillas. Cuestiones Conflictivas en la Actual Regulación de los Delitos de Pornografia Infantil. In: GONZÁLEZ, Javier García (Coordenador). **Ciberacoso: la tutela penal de la intimidad, la integridad y la libertad sexual em Internet**. Valencia: Tirant Lo Blanch, 2010, p. 183-220.

FERRAJOLI, Luigi. **Derecho y razón: Teoría del garantismo penal**. Madrid: Editorial Trotta, 1997.

FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari**. Crimes no Meio Ambiente Digital e a Sociedade da Informação**, 2. ed., Saraiva: São Paulo, 2016.

FONSECA, Joel Pinheiro da. Conectados e Solitários: a Geração Z. **Exame**, 16 dez. 2017. Disponível em: https://exame.abril.com.br/economia/conectados-e-solitarios-a-geracao-z/. Acesso em: 09 fev. 2020.

FORTES, Carolina. Lei de Segurança Nacional não poderia ser aplicada para hackers de Moro, diz especialista. **Jovem Pan**, 27 jul. 2019. Disponível em: https://jovempan.com.br/noticias/brasil/lei-de-seguranca-nacional-nao-poderia-ser-aplicada-para-hackers-de-moro-diz-especialista.html. Acesso em: 19 out. 2020.

FRANÇA. **Agence nationale de la sécurité des systèmes**. Disponível em: https://www.ssi.gouv.fr/. Acesso em 17 mar. 2020.

FRANÇA. **Código Penal Francês**. Paris, 01 mar. 1994. Disponível em: https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719. Acesso em: 16 mar. 2020.

FRANÇA. FIC 2020: L´ANSSI plaide pour une souveranité européene en matiére de cybersecurité. **Agência Nacional de Segurança de Sistemas da Informação**. Disponível em: https://www.ssi.gouv.fr/actualite/fic-2020-lanssi-plaide-pour-une-souverainete-europeenne-en-matiere-de-cybersecurite/. Acesso em: 17 mar. 2020.

FRANÇA. **Loi n° 88-19**, du 5 janvier 1988 relative à la fraude informatique. Disponível em: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000875419&categorieLien=id. Acesso em: 25 fev. 2020.

FRANÇA. **Loi n° 2004-575**, du 21 juin 2004 pour la confiance dans l'économie numérique. Disponível em: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164. Acesso em: 24 fev. 2020.

FRANÇA. **Loi nº 2009-669**, du 12 juin 2009, Haute Autorité pour la Diffusion des Œuvres et la Protection des droits sur Internet. Disponível em: https://www.hadopi.fr/en. Acesso em: 24 fev. 2020.

FRANCISCATTO, Roberto; CRISTO, Fernando de; PERLIN, Tiago. **Redes de Computadores.** Santa Maria: Universidade Federal de Santa Maria, 2014.

FREITAS JUNIOR, Dorival. Princípio Da Legalidade (Taxatividade da Lei) Como Garantia Da Dignidade Humana. **Centro Universitário Salesiano de São Paulo**, 2016. Disponível em: http://unisal.br/hotsite/mostraderesponsabilidadesocial/wp-content/uploads/sites/11/2016/08/Artigo-Dorival-de-Freitas-Junior-T%C3%ADtulo-Princ%C3%ADpio-da-Legalidade-como-garantia_da_dignidade_humana.pdf. Acesso em: 19 out. de 2020.

FUENTE, Elvira Tejada de la. Novedades en la Tipificación de Determinados Delitos Vinculados a la Criminalidad Informática en el Código Penal Español; Evolución Legislativa y Adaptación a la Normativa Internacional. In: DUPUY, Daniela (Direção); KIEFER, Mariana (Coordenação). **Cibercrimen: Aspectos de Derecho penal y procesal penal. Cooperación Internacional. Recolección de evidencia digital. Responsabilidad de los provedores de servicios de Internet**. Buenos Aires: Editorial B de F, 2019, p. 33-57.

GALLARDO-ROSALES, Rodolfo. **La Deep Web**. Disponível em: http://gallardo.mx/wp/?p=2391. Acesso em: 10 dez. 2019.

GÁLIK, Slavomí; TOLNAIOVÁ, Sabína Gáliková. Cyberspace as a New Existential Dimension of Man. In: ABU-TAIEH, Evon. **Cyberspace**. 2019, p. 1-13.

GARCIA, Rafael de Deus. Os direitos à privacidade e à intimidade: origem, distinção e dimensões. **Revista da Faculdade de Direito do Sul de Minas**. Pouso Alegre, 2018, v. 34, p. 1-26.

GARCÍA, Hugo. El Denominado "Grooming": una Nueva Modalidad de Acoso en la Era Digital. In: In: RIQUERT, Marcelo A. (direção); SUEIRO, Carlos Christian (coordenação). **Sistema penal e informática: ciberdelitos, evidencia digital, TICS 2**. Buenos Aires: Hammurabi, 2019, p. 283-290.

GIBSON, William. **Neuromancer**. São Paulo: Editora Aleph, ed. 5, 2016.

GLANCY, Dorothy J. Privacy and the Other Miss M. **Santa Clara Law Digital Commons**, Santa Clara, 1989/1990, n. 10, p. 401-440.

GLANCY, Dorothy J. The Invention of the Right to Privacy. **Arizona Law Review**. Tucson, 1979, v. 21, n. 1, p. 1-39.

GOMES, Helton Simões. 'Efeito WhatsApp' e crise 'matam' 10 milhões de linhas de celular no Brasil. **G1**, 08 dez. 2015. Disponível em: http://g1.globo.com/tecnologia/noticia/2015/12/efeito-whatsapp-e-crise-matam-10-milhoes-de-linhas-de-celular-no-brasil.html. Acesso em: 10 dez. 2019.

GÓMEZ-DIAGO, Glória. Cyberspace and Cyberculture. In Kosut, M. & Golson, J. Geoffrey (editores). **Encyclopedia of Gender in Media**. Thousand Oaks, SAGE Reference Publication, 2012, p. 1-5.

GOUVÊA, Sandra. **O Direito na Era Digital: Crimes Praticados por meio da Informática**. Rio de Janeiro: Mauad, 1997,

GOV.UK. **National Cyber Security Strategy 2016 to 2021**. Disponivel em: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021. Acesso em: 24 fev. 2020.

GUGERLI, David; ZETTI, Daniela. Computer history – The pitfalls of past futures. **Preprints zur Kulturgeschichte der Technik**. Zurique, 2019, n. 33, p.1-21.

GRIFFIN, Andrew. Tim Berners-Lee: creator of the web reveals plan to stop internet turning into 'digital dystopia'. **The Independent**, 25 nov. 2019. Disponível em: https://www.independent.co.uk/life-style/gadgets-and-tech/news/tim-berners-lee-internet-web-contract-founder-facebook-google-a9216686.html. Acesso em: 04 jan. 2020.

HACKER que roubou fotos de Scarlett Johansson pega 10 anos de prisão. **G1**, 17 dez. 2012. Disponível em http://g1.globo.com/tecnologia/noticia/2012/12/hacker-que-roubou-fotos-de-scarlet-johansson-pega-10-anos-de-prisao.html. Acesso em: 01 mar. 2020.

HACKERS que roubaram fotos de Carolina Dieckmann são presos. **Techmundo**, 14 maio 2012. Disponível em https://www.tecmundo.com.br/ataque-hacker/23514-*hackers*-que-roubaram-fotos-de-carolina-dieckmann-sao-presos.htm. Acesso em: 01 mar. 2020.

HENRY, Alan. The Difference Between Antivirus and Anti-Malware (and Which to Use). **Lifehacker**, 21 ago. 2013. Disponível em: https://lifehacker.com/the-difference-between-antivirus-and-anti-malware-and-1176942277. Acesso em: 14 fev. 2020.

HÖLTGEN, Stefan. Fifty years in home computing, the digital computer and its private use(er)s. **International Journal of Parallel, Emergent and Distributed Systems**. Londres, mar. 2019, p. 170-184.

HOMEM que clonou celular de Rollemberg irá prestar serviços à comunidade. **Jornal de Brasília**, 24 jan. 2017. Disponível em: https://jornaldebrasilia.com.br/cidades/homem-que-clonou-celular-de-rollemberg-ira-prestar-servicos-a-comunidade/. Acesso em: 17 mar. 2020.

HONEYPOT, **Collins Dictionary**, HarperCollins Publishers LLC, 2020. Disponível em: https://www.collinsdictionary.com/dictionary/english/honeypot. Acesso em: 20 out. 2020.

IANNELLO, Romina S.; VELTANI, J. Darío. La "Pornovenganza" en el Derecho Penal Argentino. In: DUPUY, Daniela (direção); KIEFER, Mariana (Coordenação). **Cibercrimen II: Nuevas conductas penales y contravencionales; Inteligencia artificial aplicada al Derecho Penal y procesal penal; Novedosos médios probatórios para recolectar evidencia digital; Cooperación internacional y victimología**. Buenos Aires: Editorial B de F, 2018, p. 75-93.

İLTER, Tuğrul. The Otherness of Cyberspace, Virtual Reality and Hypertext. In: ABU-TAIEH, Evon. **Cyberspace**. Londres: IntechOpen, 2019, p. 635-646.

IMPRESSÃO à distância é o ponto-chave das novas multifuncionais da HP. **Correio Braziliense**, 26 out. 2010. Disponível em: https://www.correiobraziliense.com.br/app/noticia/tecnologia/2010/10/26/interna_tecnologia, 219997/impressao-a-distancia-e-o-ponto-chave-das-novas-multifuncionais-da-hp.shtml. Acesso em: 09 fev. 2020.

INNOVATIVE Aspects of the BINAC, the First Electronic Computer Ever Sold. **Jeremy Norman's History of Science**. Disponível em: http://historyofinformation.com/detail.php?entryid=844. Acesso em: 22 jan. 2020.

INSTITUCIONAL. **SaferNet Brasil**. Disponível em: https://new.safernet.org.br/content/institucional. Acesso em: 13 mar. 2020.

INTERNET alimenta abusos contra mulheres, alerta seu inventor. **Istoé**, 12 mar. 2020. Disponível em: https://istoe.com.br/internet-alimenta-abusos-contra-mulheres-alerta-seu-inventor/. Acesso em: 12 mar. 2020.

INTERNET facilita tráfico de drogas, diz relatório. **BBC**, 27 fev. 2002. Disponível em: https://www.bbc.com/portuguese/ciencia/020227_internetmtc1.shtml. Acesso em: 16 fev. 2020.

ITÁLIA. **Código Penal Italiano – Decreto 19 ottobre 1930, n. 1398**, Roma, 19 out. 1930. Disponível em: https://www.altalex.com/documents/codici-altalex/2014/10/30/codice-penale. Acesso em: 24 fev. 2020.

ITÁLIA. **Constituição da República Italiana**. Roma, 22 dez. 1947. Disponível em: https://www.senato.it/documenti/repository/istituzione/costituzione.pdf. Acesso em: 16 mar. 2020.

ITÁLIA. **Decreto Legislativo 29 dicembre 1992, n. 518.** Disponível em: https://www.gazzettaufficiale.it/eli/id/1992/12/31/092G0565/sg. Acesso em 24 fev. 2020.

ITÁLIA. **Legge 23 dicembre 1993 n. 547**. Disponível em: https://www.gazzettaufficiale.it/atto/serie_generale/caricaDettaglioAtto/originario?atto.dataPubblicazioneGazzetta=1993-12-30&atto.codiceRedazionale=093G0633&elenco30giorni=false. Acesso em: 24 fev. 2020.

JACOBY, Nicole. Redefining the right to be let alone: privacy rights and the constitutionality of technical surveillance measures in Germany and the United States. **Georgia Journal of International and Comparative Law**. Atenas, 2007, v. 35, n. 3, p. 433-493.

JAISHANKAR, Karuppannan; CHANDRA, R. Rochin. **Space Transition Theory Simplified**. Disponível em: https://www.linkedin.com/pulse/space-transition-theory-simplified-r-rochin-chandra-k-k-jaishankar/. Acesso em: 19 fev. 2020.

JESUS, Damásio de; MILAGRE, José Antonio. **Manual de Crimes Informáticos**. São Paulo: Editora Saraiva, 2016.

JUÍZA diz que Facebook trata autoridade judicial 'com deszelo'. **G1**, 19 jul. 2016. Disponível em: http://g1.globo.com/tecnologia/noticia/2016/07/whatsapp-veja-perguntas-em-ingles-que-o-facebook-enviou-justica.html. Acesso em: 13 mar. 2020.

KANT, Immanuel. **Metaphysical Elements of Justice: Part I of the Metaphysics of Morals**. Tradução de John Ladd. Cambridge: Hackett Publishing Company, 2 ed., 1999,

KADIR, Nadiah Khaeriah; JUDHARIKSAWAN; Maskun. Terrorism and Cyberspace: A Phenomenon of Cyber-Terrorism as Transnational Crimes. **Fiat Justisia**, Lampung: 2019, v. 13, n. 4, p. 333-344.

KEY Events in the Development of the UNIVAC, the First Electronic Computer Widely Sold in the United States. **Jeremy Norman's History of Science**. Disponível em http://historyofinformation.com/detail.php?id=659. Acesso em: 22 dez. 2019.

KIEFER, Mariana. Dano Informático. In: DUPUY, Daniela (Direção); KIEFER, Mariana (Coordenação). **Cibercrimen: Aspectos de Derecho penal y procesal penal. Cooperación Internacional. Recolección de evidencia digital. Responsabilidad de los provedores de servicios de Internet**. Buenos Aires: Editorial B de F, 2019, p. 313-344.

KURTZ, João. Linux: Linux: Tudo o que você precisa saber antes de começar a usar. **TechTudo**, 24 mar. 2015. Disponível em: https://www.techtudo.com.br/noticias/noticia/2015/03/linux-tudo-o-que-voce-precisa-saber-antes-de-comecar-usar.html. Acesso em: 13 abril de 2020.

LACERDA, Ricardo. O Portal de Drogas da Deep Web. **Superinteressante**, 17 maio 2018. Disponível em: https://super.abril.com.br/comportamento/o-portal-de-drogas-da-deep-web/. Acesso em: 16 fev. 2020.

LAVADO, Thiago. Uso da Internet no Brasil Cresce e 70% da População está Conectada. **G1 – O Portal de Notícias da Globo**, 28 ago. 2019. Disponível em https://g1.globo.com/economia/tecnologia/noticia/2019/08/28/uso-da-internet-no-brasil-cresce-e-70percent-da-populacao-esta-conectada.ghtml. Acesso em: 26 nov. 2019.

LAZIC, Ljubomir. Benefit From AI In Cybersecurity. **The 11th International Conference on Business Information Security (BISEC-2019).** Belgrado, Sérvia, out. 2019.

LEAL, Luziane de Figueiredo Simão. **Os Crimes contra os Direitos da Personalidade na Internet: Violações e Reparações de Direitos Fundamentais nas Redes Sociais**. Curitiba: Juruá, 2015.

LEÃO, Anabela Costa; NEVES, Inês; COUTINHO, Juliana Ferraz; NETO, Luísa (Coords.). **Declaração Universal dos Direitos Humanos | Convenção Europeia dos Direitos Humanos: Anotações pelos estudantes da Faculdade de Direito da Universidade do Porto**. Porto: Universidade do Porto, 2019.

LEE, John A. N. **Computer Pioneers**. Los Alamitos: IEEE Computer Society Press, 1995.

LEE, John A. N.; IMPAGLIAZZO, John. Using Computer History to Enhance Teaching. In: LEE, John A. N.; IMPAGLIAZZO, John. **History of Computing in Education. Boston: Spring Science Business & Media**, p. 165-175.

LEI brasileira ainda é insuficiente para punir *hackers*. **Jornal O Sul**, 07 jul. 2019. Disponível em: https://www.osul.com.br/a-lei-brasileira-ainda-e-insuficiente-para-punir-*hackers*/. Acesso em: 17 mar. 2020.

LEVY, Pierre. **Cibercultura**. São Paulo: Ed. 34, 1999.

LEVY, Steven. **Hackers: Heroes of The Computer Revolution**. Nova York: Dell Publishing, 1984.

LI, Johannes Xingan. Cyber Crime and Legal Countermeasures: A Historical Analysis. **International Journal of Criminal Justice Sciences**. Ahmedabad, 2017, v. 12, p. 196-207.

LICKS, Otto Banho; ARAÚJO JÚNIOR, João Marcello. Aspectos Penais dos Crimes de Informática no Brasil. **Revista do Ministério Público**. São Paulo: Nova Fase, 1994, p. 82-103.

LINUX. In: **Encyclopaedia Britannica**. Disponível em: https://www.britannica.com/technology/Linux. Acesso em: 13 abril 2020.

LUBER, Stefan. Was ist Computerkriminalität?. **Security Insider**, 14 de setembro de 2018. Disponível em: https://www.security-insider.de/was-ist-computerkriminalitaet-a-741838/. Acesso em: 07 abr. 2020.

LUCA, Javier Augusto de. Delitos Informáticos, Apuntes de 2016. In: DUPUY, Daniela (Direção); KIEFER, Mariana (Coordenação). **Cibercrimen: Aspectos de Derecho penal y procesal penal. Cooperación Internacional. Recolección de evidencia digital. Responsabilidad de los provedores de servicios de Internet**. Buenos Aires: Editorial B de F, 2019, p.7-32.

MAGALHÃES, Marcus Abreu de; SYDOW, Spencer Toth. **Cyberterrorismo: a Nova Era da Criminalidade**. Belo Horizonte: Editora D´Plácido, 2019.

MAIA, Luciano Soares. A privacidade e os princípios de proteção do indivíduo perante os bancos de dados pessoais. In: Conselho Nacional de Pesquisa e Pós- Graduação em Direito (CONPEDI). **Anais do XVI Congresso Nacional do Conpedi**. Florianópolis: Fundação Boiteux, 2008, p. 453-466.

MALAQUIAS, Roberto Antônio Darós. **Crimes Cibernéticos e Prova: a Investigação Criminal em Busca da Verdade**. Curitiba: Juruá, 2015.

MARCOLIN, Neldson. Máquina de Calcular: Invenção do matemático francês Blaise Pascal completa 360 anos. **Pesquisa FAPESP**, maio 2002, ed. 75, p. 8-9.

MARSON, Stephen M. A Selective History of Internet Technology and Social Work, **Journal of Technology in Human Services**. Abingdon, 1997, v. 14, p. 35-49.

MARTÍNEZ, Marcos. Como as 'fake news' no WhatsApp levaram um povoado a linchar e queimar dois homens inocentes. **BBC**, 14 nov. 2018. Disponível em: https://www.bbc.com/portuguese/salasocial-46206104. Acesso em: 18 fev. 2020.

MAUES, Gustavo Brandão Koury; DUARTE, Kaique Campos; CARDOSO, Wladirson Ronny da Silva. Crimes Virtuais: Uma análise sobre a adequação penal brasileira. **Revista Científica da FASETE**. Paulo Afonso, 2018, p. 166-180.

MEDRANO, Marcia Muñoz de Alba. La protección de la persona frente a las tecnologías de la comunicación. In: SALGADO, David Cienfuegos; VÁZQUEZ, Maria Carmen Macías (Coords.). **Estudios em homenaje a Marcia Muñoz de Alba Medrano**. Cidade do México: Universidad Autonóma del México, 2006, p. 1-11.

MENDES, Priscilla. Dieckmann foi chantageada em R$ 10 mil por fotos, diz advogado. **G1**, 05 maio 2012. Disponível em: http://g1.globo.com/tecnologia/noticia/2012/05/dieckmann-foi-chantageada-em-r10-mil-devido-fotos-diz-advogado.html. Acesso em: 01 mar. 2020.

MIJWIL, Maad M. **History of Artificial Intelligence**, abr. 2015. Disponível em: https://www.researchgate.net/publication/322234922_History_of_Artificial_Intelligence. Acesso em: 20 dez. 2019.

MIJWIL, Maad M. **History of Computer**, mar. 2018. Disponível em: https://www.researchgate.net/publication/324418120_History_of_the_Computer. Acesso em: 18 dez. 2019.

MINAHIM, Maria Auxiliadora de Almeida. Legitimação do Direito Penal por Princípios Reconhecidos e Inseridos nas Constituições de Estados Democráticos de Direito. **Revista da Faculdade Mineira de Direito**. Belo Horizonte, 2017, v. 20, n. 40, p. 70-90.

MINISTÉRIO PÚBLICO FEDERAL. **Denúncia em face de Walter Delgatti Neto, Gustavo Henrique Elias Santos, Thiago Eliezer Martins Santos, Danilo Cristiano Marques, Suelen Priscila De Oliveira, Luiz Henrique Molição e Glenn Edward Greenwald**. Procuradoria da República no Distrito Federal, Brasília, 20 jan. 2020. Disponível em: http://www.mpf.mp.br/df/sala-de-imprensa/docs/denuncia-spoofing. Acesso em: 03 maio 2020.

MIR PUIG, Santiago. **Derechos Humanos y Limites del Derecho Penal**. Disponível em: https://www.ehu.eus/documents/1736829/2019658/19+-+Derechos+humanos+limites.pdf. Acesso em: 29 set. 2019.

MIRÓ LLINHARES, Fernando. La Respuesta Final al Ciberfraude: Especial atención a la responsabilidad de los muleros del phishing. **Revista Electrónica de Ciencia Penal y Criminología**. Granada, 2013, n. 15, p. 12-56.

MOCHETTI, Karina. The Impact of Women in Computer Science History: A Post-War American History. **Transversal International Journal for the Historiography of Science**. Belo Horizonte, 2019, n. 6, p. 65-89.

MOLICA, Fernando; RESENDE, Leandro. Glenn Greenwald revela diálogo com fonte de mensagens vazadas. **Veja**, 26 jul. 2019. Disponível em: https://veja.abril.com.br/politica/glenn-greenwald-revela-dialogo-com-fonte-de-mensagens-vazadas/. Acesso em: 01 mar. 2020.

MONTIEL, Irene; AGUSTINA, José R. Victimización Sexual de Menores A Través de las TIC. **Cibercrimen II: Nuevas conductas penales y contravencionales; Inteligencia artificial aplicada al Derecho Penal y procesal penal; Novedosos médios probatórios para recolectar evidencia digital; Cooperación internacional y victimología**. Buenos Aires: Editorial B de F, 2018, p. 405-439.

MUNGO, Paul; CLOUGH, Bryan. **Approaching zero: the extraordinary underworld of *hackers*, phreakers, virus writers, and keyboard criminals**. Nova York: Random House Inc., 1993.

MUNIAGURRIA, Pablo H. Gris; CHERÑAVSKY, Nora A.; MOREIRA, Diógenes. "Phishing": Abordagem do Fenômeno desde a Prevenção e a Investigação. In: In: RIQUERT, Marcelo A. (direção); SUEIRO, Carlos Christian (coordenação). **Sistema penal e informática: ciberdelitos, evidencia digital, TICS 2**. Buenos Aires: Hammurabi, 2019, p. 117-134.

MUNJAL, Meenaakshi N. **Ethical Hacking: an Impact on Society**. Disponível em: https://www.researchgate.net/publication/262726769_ETHICAL_HACKING_AN_IMPACT_ON_SOCIETY. Acesso em: 17 ago. 2019.

MINISTÉRIO PÚBLICO DO ESTADO DO MARANHÃO. MPMA cria campanha para alertar sociedade sobre ofensas em redes sociais. **Ministério Público do Estado do**

Maranhão. 27 mar. 2018. Disponível em: https://www.mpma.mp.br/index.php/lista-de-noticias-gerais/11/14254. Acesso em: 08 fev. 2020

MURRAY, Andrew. The dark web is not just for pedophiles, drug dealers and terrorists. **The Independent**, Londres, 12 dez. 2014. Disponível em: https://www.independent.co.uk/voices/comment/the-dark-web-is-not-just-for-paedophiles-drug-dealers-and-terrorists-9920667.html. Acesso em: 11 dez. 2019.

NELSON, Theodore Holm. **Home Page of Ted Nelson**. Disponível em: http://ted.hyperland.com/. Acesso em: 17 fev. 2020.

NOMURA, Leandro. 'Crime na internet é ferida aberta', diz mãe sobre fotos nuas vazadas pelo ex. **Folha de São Paulo**, 21 maio 2017. Disponível em: https://www1.folha.uol.com.br/empreendedorsocial/minhahistoria/2017/05/1885458-crime-na-internet-e-ferida-aberta-diz-mae-sobre-fotos-nuas-vazadas-pelo-ex.shtml. Acesso em: 18 fev. 2020.

NOVELLI, Rodrigo Fernandes. A teoria do garantismo penal e o princípio da legalidade. **Revista Jurídica UNIGRAN**. Dourados, jan./jun. 2014, v. 16, n. 31, p. 119-129.

OMS cria canal no WhatsApp para informar avanço e tirar dúvidas sobre coronavírus. **Folha de São Paulo**, 24 mar. 2020. Disponível em https://www1.folha.uol.com.br/equilibrioesaude/2020/03/oms-cria-canal-no-whatsapp-para-informar-avanco-e-tirar-duvidas-sobre-coronavirus.shtml. Acesso em: 23 ago. 2020.

ORGANIZAÇÃO DOS ESTADOS AMERICANOS. **Quem Somos**. Disponível em: http://www.oas.org/pt/sobre/quem_somos.asp. Acesso em: 14 mar. 2020.

PALAZZI, Pablo A. **Delitos Contra la Intimidad Informática**. Buenos Aires: Colección Derecho y Tecnología. 2019.

PALMA, Gabriel; BOMFIM, Camila. Operação prende 39 em combate à pornografia infantil no Brasil e em mais 6 países. **G1**, 04 set. 2019. Disponível em: https://g1.globo.com/df/distrito-federal/noticia/2019/09/04/operacao-combate-pornografia-infantil-no-brasil-e-em-outros-6-paises.ghtml. Acesso em: 17 fev. 2020.

PAOLLA Oliveira tem fotos íntimas vazadas. **Revista Cláudia**, 02 mar. 2018. Disponível em: https://claudia.abril.com.br/famosos/globo-descobre-responsavel-divulgacao-fotos-intimas-de-paolla-oliveira/. Acesso em: 10 mar. 2020.

PARANAIBA, Guilherme. Estudante de química oferecia “cardápio” de drogas e orientações pela Internet. **Estado de Minas Gerais**, 28 nov. 2018. Disponível em: https://www.em.com.br/app/noticia/gerais/2018/11/28/interna_gerais,1008758/estudante-de-quimica-oferecia-cardapio-de-drogas-pela-internet.shtml. Acesso em: 16 fev. 2020.

PARENTS have right to access dead daughter's Facebook profile, German court rules. **Reuters**, 12 de julho de 2018. Disponível em https://www.reuters.com/article/facebook-privacy-germany/parents-have-right-to-access-dead-daughters-facebook-profile-german-court-rules-idUSL8N1U82E7. Acesso em: 15 mar. 2020.

PERGUNTAS frequentes sobre canais. **Telegram**. Disponível em: https://telegram.org/faq_channels/br Acesso em: 23 ago. 2020.

PERU. **Código Penal Peruano**. Disponível em: http://spij.minjus.gob.pe/content/publicaciones_oficiales/img/CODIGOPENAL.pdf. Acesso em: 26 fev. 2020.

PERU. **Ley N° 27309 de 17 de julio de 2000. Modifícase el Título V del Libro Segundo del Código Penal, promulgado por Decreto Legislativo Nº 635**. Disponível em: https://www.gob.pe/institucion/pcm/normas-legales/292284-27309. Acesso em: 26 fev. 2020.

PETRONE, Daniel; BASSO, Mariana; EMILIOZZI, Agustina. Phishing Attacks: Problemáticas de su Recepción em el Ordenamento Local y Nuevos Desafíos. In: DUPUY, Daniela (Direção); KIEFER, Mariana (Coordenação). **Cibercrimen: Aspectos de Derecho penal y procesal penal. Cooperación Internacional. Recolección de evidencia digital. Responsabilidad de los provedores de servicios de Internet**. Buenos Aires: Editorial B de F, 2019, p. 277-290.

PINEDA, Francisco Almenar. **Ciberdelincuencia: Teoría y Práctica**. Curitiba: Juruá Editorial, 2018.

PINHEIRO, Patrícia Peck Garrido. A responsabilidade no uso das mídias sociais em nossas comunidades. In: PINHEIRO, Patrícia Peck Garrido (Coordenadora). **Direito Digital Aplicado 3.0**. São Paulo: Thomson Reuters Brasil, 2018, p. 248-250.

PINO, Martim Manuel; GONÇALVES, Diego Marques. Os direitos à intimidade e à privacidade em face aos mecanismos de coleta de dados pessoais na rede mundial de computadores. **Revista de Propriedade Intelectual, Direito Contemporâneo e Constituição**. Aracaju, 2017, v. 11, n. 03, p. 1-20.

PORTUGAL. **Lei n.º 109/91.** Lei da criminalidade informática. Disponível em: https://dre.pt/pesquisa/-/search/674438/details/maximized. Acesso em: 24 fev. 2020.

POLÍCIA ouve empresa de informática sobre fotos de Carolina Dieckmann. **G1**, 07 maio 2012. Disponível em: http://g1.globo.com/rio-de-janeiro/noticia/2012/05/policia-ouve-empresa-de-informatica-sobre-fotos-de-carolina-dieckmann.html. Acesso em: 01 mar. 2020.

PRADO, Luiz Regis. **Curso de Direito Penal Brasileiro: parte geral e parte especial**. Rio de Janeiro: Editora Forense, 17a. ed. 2019.

PRASAD, M. R. Murali. Deep Web: Librarian's Perspective. **PEARL - A Journal of Library and Information Science**. Porto, out-dez. 2017, v. 11, n. 4, p. 418-423.

PRAZERES, Leandro. PF indicia seis hackers por invasão de celulares que atingiu Sergio Moro. **O Globo**, Brasília, 19 dez. 2019. Disponível em https://oglobo.globo.com/brasil/pf-indicia-seis-*hackers*-por-invasao-de-celulares-que-atingiu-sergio-moro-24147902. Acesso em: 01 mar. 2020.

PROTESTOS na Internet: Conheça 7 casos recentes de ativismo hacker. **Canaltech**, 21 set. 2017. Disponível em: https://canaltech.com.br/internet/protestos-na-internet-conheca-7-casos-recentes-de-ativismo-hacker-100796/. Acesso em: 01 mar. 2020.

PUTROV, Sergiy; IVANOVA, Galina. Cyberculture: Change and Rehabilitation the Body. **Philosophy and Cosmology**. Pereyaslav, 2018, v. 21, p. 116-122.

QUANTO tempo você precisa ficar longe do celular e das redes para uma 'desintoxicação digital' efetiva?. **BBC**, 27 mar. 2017. Disponível em: https://www.bbc.com/portuguese/internacional-39402166. Acesso em: 04 mar. 2020.

RAYMOND, Eric Steven. **How to become a hacker**. Disponível em: http://www.catb.org/~esr/faqs/hacker-howto.html. Acesso em: 16 ago. 2019.

RAYMOND, Eric S. **The New Hacker's Dictionary**. Cambridge: Mit Press, 2000.

REEGÅRD, Kine; BLACKETT, Claire; KATTA, Vikash. The Concept of Cybersecurity Culture. **Proceedings of the 29th European Safety and Reliability Conference**. Hannover: Research Publishing, 2019, p. 4036-4043.

REIS, Maria Helena Junqueira. **Computer Crimes**. Belo Horizonte: Del Rey, 1997.

RELATÓRIO da Segurança Digital – segundo semestre de 2018. **PSafe**. Disponível em: https://www.psafe.com/dfndr-lab/wp-content/uploads/2018/08/Relat%C3%B3rio-da-Seguran%C3%A7a-Digital-no-Brasil-2-trimestre-2018.pdf. Acesso em: 13 abr. 2020.

RICHET, Jean-Loup. Free Young *Hackers* to Crackers. **International Journal of Technology and Human Interaction**. Hershey, jun.-set. 2013, p. 53-62.

ROCHA, Camilo. Tudo Conectado: entrevista com Shawn DuBravac, economista-chefe da CEA, entidade que organiza a Consumer Eletronic Show. **O Estado de São Paulo**, 08 jan. 2012. Disponível em: https://link.estadao.com.br/noticias/geral,tudo-conectado,10000036849. Acesso em: 09 fev. 2020.

RODRIGUES, Fabíola Emilin. **Tutela Penal Ambiental: Eficácia da Norma Penal em Branco**. Dissertação (Mestrado em Direito). Orientador: Marco Antonio Marques da Silva. Pontíficia Universidade Católica de São Paulo. São Paulo, 2005, 242 fls.

RODRÍGUEZ, Víctor Gabriel. **Tutela Penal da Intimidade: perspectivas da atuação penal na sociedade da informação**. São Paulo: Atlas, 2008.

SAIN, Gustavo. La Estrategia Gubernamental frente al Cibercrimen: la importância de las políticas preventivas más allá de la solución penal. In: PARADA, Ricardo Antonio (comp.). **Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet**. Buenos Aires: Erreius, 2018, p. 7-32.

SALERNO, Giulio M. A Proteção da Privacidade e a Inviolabilidade da Correspondência. **Revista da AJURIS**. Porto Alegre, dez. 2012, v. 39, n. 128, p. 355-420.

SCHMITT, Michael N. (org.). **Manual on the International Law Applicable to Cyber Warfare.** Cambridge: Cambridge University Press, 2013.

SCHMITT, Michael N. (org.). **Manual 2.0 on the International Law Applicable to Cyber Operations**. Cambridge: Cambridge University Press, 2017.

SCHMITT, Paula. Vaza Jato, Glenn Greenwald e uma coincidência intrigante – parte 3. **Poder 360**, 20 fev. 2020. Disponível: https://www.poder360.com.br/opiniao/midia/vaza-jato-glenn-greenwald-e-uma-coincidencia-intrigante-parte-3-por-paula-schmitt/. Acesso em: 01 mar. 2020.

SHIMABUKURO, Adriana; SILVA, Melissa Garcia Blagitz de Abreu e. Internet, Deep Web e Dark Web. In: SILVA, Angelo Roberto Ilha da. **Crimes Cibernéticos**. Porto Alegre: Livraria do Advogado, 2017, p. 255-270.

SIEBER, Ulrich. **Legal Aspects of Computer-Related Crime in the Information Society**, 01 jan. 1998. Disponível em: https://ec.europa.eu/archives/ISPO/legal/en/comcrime/sieber.html. Acesso em: 20 fev. 2020.

SILVA, Louise Trigo da. Legalidade e taxatividade: a necessidade de definições e os tipos abertos. **Revista Eletrônica Direito e Política do Programa de Pós-Graduação Stricto Sensu em Ciência Jurídica da UNIVALI**. Itajaí, 2012, v.7, n.2, p. 1020-1037.

SILVA, César Dario Mariano da. **Tutela Penal da Intimidade**. Curitiba: Juruá. 2015,

SILVA SANCHEZ, Jesús María. **La Expansión del Derecho Penal: aspectos de la política criminal en las sociedades postindustriales**. Madri: Civitas, 2. ed., 2001.

SOLITUDE. In: **Dicionário Online de Português**. Disponível em: https://www.dicio.com.br/solitude/. Acesso em: 04 mar. 2020.

SYDOW, Spencer Toth. **Crimes Informáticos e Suas Vítimas**. 2 ed., São Paulo: Saraiva, 2015.

SYDOW, Spencer Toth. **Curso de Direito Penal Informático – Partes Geral e Especial**. Salvador: JusPodium, 2020.

SYDOW, Spencer Toth. El Impacto de la Informática en El Sistema Jurídico Penal Brasileiro. In: RIQUERT, Marcelo A. (direção); SUEIRO, Carlos Christian (coordenação). **Sistema penal e informático: ciberdelitos, evidencia digital, TICS**. Buenos Aires: Hammurabi, 2019, p. 285-295.

SYDOW, Spencer Toth; CASTRO, Ana Lara Camargo de. **Exposição Pornográfica Não consentida na Internet: da Pornografia de Vingança ao Lucro**. Belo Horizonte: Editora D´Plácido, 2017.

TADDEO, Mariarosaria. Is Cybersecurity a Public Good? **Minds and Machines - Journal for Artificial Intelligence, Philosophy and Cognitive Science**. Oxford, 2019, v. 29, p. 349-354.

TEMPERINI, Marcelo; MACEDO, Maximiliano. Nuevas Herramientas de Investigación Penal: El Agente Encubierto Digital. In: DUPUY, Daniela (Direção); KIEFER, Mariana (Coordenação). **Cibercrimen: Aspectos de Derecho penal y procesal penal. Cooperación Internacional. Recolección de evidencia digital. Responsabilidad de los provedores de servicios de Internet**. Buenos Aires: Editorial B de F, 2019, p. 481-514.

THE Apple iPad is released. **Computer History Museum**. Disponível em: https://www.computerhistory.org/timeline/2010/. Acesso em: 23. dez. 2019.

TRANSISTOR-Transistor Logic (TTL). In: **Technopedia**. Edmonton: Janalta Interactive, 2016. Disponível em: https://www.techopedia.com/definition/3057/transistor-transistor-logic-ttl. Acesso em: 02 de maio de 2020.

TRIBUNAL EUROPEU DE DIREITOS HUMANOS. **Case of Benedik v. Slovenia (Application no. 62357/14)**. Estrasburgo, 24 jul. 2018. Disponível em: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-182455%22]}. Acesso em: 17 mar. 2020.

TRIBUNAL SUPERIOR DO TRABALHO. **Pode ou não Pode: O empregador monitorar e-mail corporativo de trabalhadores**. Disponível em: http://www.tst.jus.br/radio-destaques/-/asset_publisher/2bsB/content/pode-ou-nao-pode-o-empregador-monitorar-e-mail-corporativo-de-trabalhadores. Acesso em: 24 abr. 2020.

TRINDADE, Rodrigo. Como WhatsApp foi de inimigo a queridinho das operadoras. **Uol**, 05 jun. 2019. Disponível em: https://www.uol.com.br/tilt/noticias/redacao/2019/06/05/tentaram-parar-inovacao-como-whatsapp-matou-sms-e-deu-licao-a-operadoras.htm. Acesso em: 23 dez. 2019.

ULBRICH, Henrique Cesar; DELLA VALLE, James. **Universidade H4ck3r**, 4. ed. São Paulo: Digerati Books. 2004.

UNITED KINGDOM. **National Cyber Security Strategy 2016 to 2021**. Disponível em: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021. Acesso em: 24 fev. 2020.

UNITED KINGDOM. **Information Comissioner`s Office**. Disponível em: https://ico.org.uk/. Acesso em: 11 abr. 2020.

UNITED NATIONS OFFICE ON DRUGS AND CRIME. **Comprehensive Study on Cybercrime**. Viena, fev. 2013.

USO de apps de bate-papo triplica em 2013, diz consultaria. **G1**, 13 jan. 2014. Disponível em: http://g1.globo.com/tecnologia/tem-um-aplicativo/noticia/2014/01/uso-de-apps-de-bate-papo-triplica-em-2013-diz-consultoria.html. Acesso em: 22 dez. 2019.

VANNUCHI, Camilo. O direito à comunicação e os desafios da regulação dos meios no Brasil. **Galaxia**. São Paulo, 2018, n. 38, p. 167-180.

VERVERIS, Vasilis. Demistifying the Dark Web. **XRDS**. Nova York, 2018, v. 24, n.4, p. 16-19.

VIANNA, Túlio Lima. **Fundamentos de Direito Penal Informático: do acesso não autorizado a sistemas computacionais**. São Paulo: Forense, 2003

WARREN, Samuel D.; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**. Cambridge, 1890, v. 4, n. 5, p. 193-220.

WHAT is cyber warfare?. IT Pro, 16 mar. 2020. Disponível em: https://www.itpro.co.uk/security/28170/what-is-cyber-warfare. Acesso em: 14 abr. 2020.

WHATSAPP bloqueado: Relembre todos os casos de suspensão do app. **G1**, São Paulo, 19 jul. 2016. Disponível em: http://g1.globo.com/tecnologia/noticia/2016/07/whatsapp-bloqueado-relembre-todos-os-casos-de-suspensao-do-app.html. Acesso em: 12 mar. 2020.

WHATSAPP bloqueado: operadoras são intimadas a barrar app no país por 48h. **G1**, São Paulo, 16 dez. 2015. Disponível em: http://g1.globo.com/tecnologia/noticia/2015/12/operadoras-sao-intimadas-bloquear-whatsapp-no-brasil-por-48-horas.html. Acesso em: 12 mar. 2020.

WILLIAMS, Michael R. The Origins, Uses, and Fate of the EDVAC. **IEEE Annals of the History of Compicting**, 1993, v. 15, n.1, p. 22-38.

WOLOSZYN, André Luis. Ciberespionagem: Entraves na Apuração de Provas e Responsabilização no Processo Penal. In: BRASIL, Ministério Público Federal. **Crimes Cibernéticos**. Brasília: 2018, p. 134-155.

ZANINI, Leonardo Estevam de Assis. A proteção da imagem e da vida privada na França. **Revista Brasileira de Direito Civil**. Belo Horizonte, 2018, v. 16, p. 57-73.